UNIFORMED SERVICES UNIVERSITY OF THE HEALTH SCIENCES

SUBJECT: Information Technology Policies and Procedures at the Uniformed Services University of the Health Sciences (USU) and the Armed Forces Radiobiology Research Institute (AFRRI)

Instruction 7900

(CIO)

ABSTRACT

JUN 3 2015

This Instruction establishes policies, assigns responsibilities, and provides procedures related to the acquisition, maintenance, security, and use of information technology equipment and systems at the Uniformed Services University of the Health Sciences (USU).

A. Reissuance and Purpose. This instruction replaces USU Instruction 7900, dated July 2005, and establishes policies and procedures for Information Technology (IT) equipment, software, related systems, and services including acquisition, installation, modification, utilization, security, and inventory.

B. References. *See Enclosure 1.*

C. Applicability. This Instruction applies to all faculty, staff, students, contractors, individuals, and groups that utilize the USU Information Technology resources associated with the USUMIL (NIPRNet) or USUEDU (Commercial) networks.

D. Policy. The following paragraphs provide University policy on specific topics:

1. Authorized Usage. The Information Technology Systems of the University are government-owned and subject to the rules and regulations of the Federal Government and the Department of Defense (DoD). Usage is granted to individuals and groups that have an established relationship with the University. Use of Government Communication Systems for personal communications must be kept to a minimum so as not to over burden the communication systems and not impact the employee's work performance. In the event of abuse, an employee's use of Government systems may be entirely withdrawn (*See Addendum D – Employee Behavior*). This is generally accomplished by the assignment of accounts, use of telephones, e-mail, network connections, databases, information systems, and access to the internet. All personnel must complete the following:

a. DD 2875, Systems Account Access Request Form.

b. DoD Cyber Awareness Challenge.

c. Signed USU Computer User Agreement as a condition of issuance of accounts. All accounts are reviewed and approved by the Cyber Security Branch. All account requests are processed through the Customer Support Division (CSD) Helpdesk prior to granting access to the USU Network Resources.

2. IT Property and Equipment. Billeted faculty, staff, and contractors, who are assigned to USU, or its official extensions, are provided a computer system to perform daily routine office automation tasks. Due to the escalating cost of maintaining systems, cyber security requirements, and in recognition of an increasingly mobile work force, USU will provide either one desktop or one laptop computer with docking station to personnel based on individual mission needs. Multiple systems purchased with O&M funds, simply to accommodate travel or telework, is not authorized. *(See Addendum T – Procurement of Desktop and Laptop Computing Systems)*

3. Acquisition, Installation, Maintenance, and Replacement of Desktop Computers.

a. **Acquisition** - Standards for desktop systems are established and/or reviewed annually by the USU Change Control Board (CCB). These standard systems are generally provided through leasing and/or purchase arrangements which enable system standardization, ongoing budget planning, and automated technology refurbishment. When funds permit, additional computers are purchased to supplement the leasing-purchase program. Priorities for the provision of standard computer systems are established by the CCB. Non-standard computer requirements may be met with activity resources (including external grant and contract funds as appropriate), or referred to the unfunded equipment review process. Non-standard systems which will be connected to the network, or communicate in any manner with other USU systems, must be approved by the CCB and configured to meet published DoD Cyber Security standards.

b. **Installation** - Installation of all systems to include standard, non-standard, contractor, etc., is performed by the CSD Helpdesk and includes the transfer of working files from the system being replaced to the new system. In addition, requesting activities are expected to provide resources for funding unplanned network extension costs.

c. **Maintenance** - On-site maintenance will be purchased with all IT systems. The CSD Helpdesk will be responsible for arranging on-site maintenance for the standard systems and other systems under their management, as appropriate. Maintenance for external systems must be coordinated with the CSD Helpdesk prior to performance of the maintenance. A log will be maintained in USU Service Desk application by the CSD Helpdesk for tracking purposes.

d. **Replacement** – Standard systems will be replaced as part of the system life cycle on a three to four-year life cycle for laptops and desktops. It is the responsibility of the individual activity to fund for the replacement of non-standard systems at the end of its life cycle. Non-standard systems that do not meet the life cycle requirements are not authorized to connect to the networks. When the retention of an existing system is requested, in addition to the receipt of a newly issued system, the exception must be approved by the CCB. University-owned systems

that are replaced will be turned into the Property Management Office for disposal. All systems must be wiped *IAW Addendum B, Sanitization and Disposal Policy*. Reassignment will follow the guidelines of the CCB and will be monitored by the CSD Helpdesk. (*See Addendum T – Procurement of Desktop and Laptop Computing Systems*)

4. Servers and Data Storage Systems. It is the intention of the University to centrally provide all server and data storage requirements under the management of the Network Operations and Communications (NOC) Directorate. Applications must be approved by the CCB to obtain and operate servers and related support requirements (an approval request can be submitted via the USU Service Desk by choosing category 'Acquisition Computer Equipment' or 'Server Other'). Individual computers may not be installed as network servers, or web servers, without the CCB approval. System operators of non-centralized servers and systems must be officially identified by their department chairs or activity heads, and meet DoD Certification and Accreditation (C&A) requirements. (*See Addendum Q - Servers Security Policy*)

5. Software and Operating Systems. The CCB is responsible for selecting standard operating systems and software programs for the University. These set of tools are meant to provide standardized operating systems, e-mail, internet browsers, word processing, spreadsheet, database, security, and presentation software that will be utilized by, and supported for, all University IT customers. It is recognized that non-standard software may be necessary to meet various teaching and research missions of the University, and such software may be obtained via appropriate funding source. Non-standard software may be purchased with the government credit card after receiving approval from the CCB. Requests for non-standard software must be submitted through the USU Service Desk online application. Any software intended to operate on multiple systems or over the network, must receive CCB approval. It is the responsibility of the operator of these non-standard systems to ensure that they remain compatible and do not interfere with the operation of the University's standard systems or violate published DoD Cyber Security requirements. Such software may not be utilized in place of standard systems for official communications.

6. Security. The University will follow Federal IT security guidelines *(References (a), (b), and (c))* in order to protect its critical information, operating systems, and the Federal systems to which it is connected. As a University in a Federal setting, USU must recognize the need for secure, protected systems while at the same time, appreciate the necessity of communicating in an open fashion with future students, fellow scientists, and appropriate portions of the internet at large. To meet this dual role, the network must be operated at three levels of security. First, is a fully protected intranet that is open only to authorized on-campus user's. Second, a portion of the network must be reached from outside of the University, through the internet, whereby students, faculty, and other authorized users with established accounts can be verified and granted access. Third, a portion of the system must be fully open to the Internet so that we can communicate with appropriate portions of the internet at large. Appropriate passwords and user accounts, firewalls, proxy servers, router tools, traffic scanners, and related security mechanisms will be utilized by the Cyber Security Branch and server administrators to maintain a proper defense-in-depth security posture. Specific Cyber Security Guidelines will be developed by the Cyber

Security Branch and reviewed by the Automated Information Systems Advisory Committee (AISAC). The Cyber Security Branch will also be responsibility for training users and system operators in appropriate security procedures.

7. Internet Usage. The internet has become an essential tool by which we communicate with prospective and current students, alumni, patients, and colleagues from the military, scientific, medical and educational communities, and the world at large. While the points of contact are extremely broad, it must be remembered that access is provided for only official business and the support of the University's missions. Usage of the internet service is therefore governed by appropriate Federal and USU policies.

8. Web Pages. The University's Web Pages, which are controlled by the University Web Master and numerous University activity web pages are managed by appointed Page Masters. As communication tools and government property, Web Pages are subject to Federal Regulations such as *references (a), (c) section 5.11, and (g)*. To a large extent, these guidelines have been summarized for the University users in USU Instruction 5202.2 (*reference (e)*).

9. E-mail Usage. The University maintains one e-mail system as its official means of communication *(reference (c))*. All personnel are responsible for communicating and receiving important announcements through this system. Privacy, security, and the rights of others should be considered in its use. The distribution of unnecessary or unofficial messages is strongly discouraged. Limited personnel will be granted the ability to send University-wide messages to every individual in the system.

10. Handicapped Access. Federal regulations control requirements for access to electronic information systems by the handicapped. Details of these requirements can be found in *reference (f)*.

11. System Upgrades. Standard systems may only be upgraded by the manufacturer through the CSD Helpdesk. However, external devices may be connected and utilized when they do not interfere with the standard operation of the computer or network systems and are approved by the CCB. The Central Processing Unit, or Mother Board, of the University-owned desktop computers may not be upgraded. However, for special purposes, and as necessary to maintain the effective use of a system, University-owned systems may be upgraded by the Technical Services Branch. All upgrades require the approval of the CCB to ensure that compatibility and minimum security requirements are maintained.

E. <u>Responsibilities</u>.

1. The President shall appoint members of the AISAC and have final approval on recommended policies.

2. Office of the Chief Information Officer (OCIO) will:

a. Supervise the overall implementation of the Information Technology systems and services within the University and monitor compliance with this Instruction.

b. Establish priorities for major AIS development and acquisition initiatives.

c. Chair the AISAC. See *Addendum A, Governance for additional CIO responsibilities.*

3. The AISAC will:

a. Be composed of members from the student body, administration, faculty, and research areas of the University.

b. Remain aware of the breadth and depth of the IT systems and services available throughout the University and conduct periodic user satisfaction surveys.

c. Determine IT requirements for current and future systems focusing special attention to the goals and objectives of the University Strategic Plan.

d. Recommend policies and procedures for obtaining, maintaining, and using University IT systems and equipment.

e. Assist the CIO in setting priorities for unfunded equipment and programming objectives.

4. The Electronic Editorial Board will periodically review web pages for format and content (at least once per year).

5. The Cyber Security Manager will:

a. Serve as principal advisor and have direct access to the Director, NOC and CIO on all USU Cyber Security matters.

b. Report all Cyber Security issues directly to the Director, NOC and CIO.

c. Ensure USU Cyber Security program requirements are properly implemented.

d. Verify and document that appropriate security tests are successfully conducted on USU computers, peripheral, ancillary devices, computer systems and networks prior to installation and when major hardware or software upgrades/ modifications occur.

e. Ensure that all Certification and Accreditation support documentation is developed, submitted, and maintained in accordance with *reference (a) – (g)*.

f. Author and provide the USU DAA with accreditation packages for all computer systems and networks within USU.

g. Ensure that all USU computer systems and networks meet security specifications for an acceptable level of risk.

h. Continuously review all System Security Accreditation Plans and complete re-accreditation actions as required.

i. Ensure that proposed system changes are reviewed, and that changes, enhancements or modifications implemented do not adversely impact system security features.

j. Ensure required contingency plans are developed and tested.

k. Ensure that all USU Information Systems user activities are monitored to verify compliance with established security policies and procedures.

l. Coordinate regularly with USU Cyber Security Officers and Network Security Officers (NSO's), to ensure that precise system-level Cyber Security support is provided and maintained for all USU computer systems and networks.

m. Author and maintain a USU Cyber Security Policies, Processes and required Standard Operating Procedures to ensure the secure design, development, operation and disposition of sensitive USU computing systems and networks.

n. Establish a comprehensive user, manager and administrator Information System Security training program within USU.

o. Ensure countermeasures, both procedural and physical, exist and are working to enhance Information System Security (e.g., key lock and terminal lock safeguards, access control and terminal/isolation barriers).

p. Review user practices and procedures for possible vulnerabilities that may pose a threat to computer security.

q. Ensure compliance with proper media/equipment control, handling, labeling, and disposition procedures.

r. Ensure "need to know" and "least privilege" rules are applied and enforced.

s. Ensure the proper handling, security control, inventory, disposition and destruction of magnetic media within USU.

t. Investigate and report actual or suspected Information System Security incidents, events or violations directly to the Director, NOC and CIO for further reporting as may be required.

u. Ensure that USU personnel who are not specifically cleared for access to sensitive or classified data are monitored and escorted at all times. Access to USU computer systems or networks processing sensitive or classified data shall be strictly controlled, monitored and limited to only those systems/networks required to fulfill individual responsibilities. Uncontrolled access to USU computer systems or networks processing classified data by un-cleared personnel is strictly prohibited. Violations must be reported immediately to the USU DAA.

6. The Cyber Security Officer will:

a. Ensure that all users have the requisite security clearances and supervisory need-to-know authorization, and are aware of their Cyber Security responsibilities before being granted access to the USU networks and DoD information systems.

b. In coordination with the Cyber Security Manager, initiate protective or corrective measures when a Cyber Security incident or vulnerability is discovered.

c. Ensure that Cyber Security and Cyber Security-enabled software, hardware, and firmware comply with appropriate security configuration guidelines.

d. Ensure that DoD information system recovery processes are monitored and that Cyber Security features and procedures are properly restored.

e. Ensure that all DoD information system Cyber Security-related documentation is current and accessible to properly authorized individuals.

f. Implement and enforce all DoD information system Cyber Security policies and procedures, as defined by its security certification and accreditation documentation.

g. Develop and maintain an organization or DoD information system-level Cyber Security program that identifies Cyber Security architecture, Cyber Security requirements, Cyber Security objectives and policies; Cyber Security personnel; and Cyber Security processes and procedures.

h. Ensure that information ownership responsibilities are established for each DoD information system, to include accountability, access approvals, and special handling requirements.

i. Ensure the development and maintenance of Cyber Security certification documentation according to DoD Instruction 8500.01 by reviewing and endorsing such documentation, and recommending action to the DAA.

j. Maintain a repository for all Cyber Security certification and accreditation documentation and modifications.

k. Ensure that all privileged users receive the necessary technical and Cyber Security training, education, and certification to carry out their Cyber Security duties.

l. Ensure that compliance monitoring occurs, and review the results of such monitoring.

m. Ensure that Cyber Security inspections, tests, and reviews are coordinated.

n. Ensure that all Cyber Security management review items are tracked and reported.

o. Ensure that incidents are properly reported to the Cyber Security Manager, DAA, and the DoD reporting chain, as required, and that responses to Cyber Security related alerts are coordinated.

p. Act as a Cyber Security technical advisor to the DAA and formally notify the DAA of any changes impacting the DoD information system's Cyber Security posture.

7. The Director, Network Operations and Communications (NOC) will:

a. Provide overall management and support for central IT computer systems, networks, and communications systems throughout the University.

b. Operate and maintain central systems and networks.

c. Recommend standards and configurations for IT systems for approval to the AISAC.

d. Review IT purchases for compatibility.

e. Provide and maintain user accounts for all authorized users.

f. Coordinate with the Logistics Division in the tracking of all University-owned IT equipment with a value over one thousand dollars.

g. Plan for, install, and maintain security systems that meet Federal guidelines within the resources provided.

h. Plan for, install, and maintain internet systems that meet Federal guidelines within the resources provided.

8. Application & Web Development (AWD) will appoint and utilize a Web Master to maintain the University Web Site and coordinate with Page Masters throughout all University activities to ensure that Federal guidelines for web site utilization are met.

9. The Customer Support Helpdesk will:

a. Provide helpdesk services during normal working hours for University personnel as resources permit.

b. Be the central point of contact for all services and equipment provided by NOC and maintain a system to track those actions.

c. Maintain contracts for both desktop software and systems and provide those products to authorized users.

10. Vice Presidents, Deans, Department Chairs and Activity Heads will:

a. Appoint IT Property Custodians for their areas of responsibility.

b. Review and approve requests for IT equipment and services originating from within their areas.

11. Individual Users will:

a. Treat information and communications systems and equipment as Federally owned and operated resources.

b. Guard passwords and procedures to maintain privacy and security.

c. Follow Federal and University guidelines for the proper use of telephones, web sites, browsers, and other communications systems.

d. Be responsible for making periodic back-up copies of official information maintained on their equipment.

e. Respect the rights of others in relation to the content of the information transported and the quantity of the resources utilized.

f. Request permission and assistance via the CSD Helpdesk before moving or making any modification to IT equipment.

F. Effective Date. This Instruction is effective immediately.

Charles L. Rice, MD
President

Enclosures:
1. References
2. Addendums

REFERENCES

(a) OMB Bulletin No. A-130.
"Transmittal Number 4 - Management of Federal Information Resources." Appendix III, "Security of Federal Automated Information Systems,' January 2000.

(b) DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information," June 2011.

(c) BUMED Field Information Security Policy Manuel, Version 1.04, May 2001.

(d) USU Instruction 5201, "Information Security Program," April 2006.

(e) USU Instruction 5202.2 Electronic Information and Communication Policies," September 2006.

(f) Final FAR Rule for Implementing Section 508 of the Rehab Act Electronic and Information Technology Accessibility for Persons with Disabilities, April 2001.

(g) DoD Directive 5500.7-R "Joint Ethics Regulation (JER), including Changes 1-7," November 2011.

Addendums

Title	Description
Addendum A	Governance
Addendum B	Sanitization
Addendum C	Incident Reporting and Response
Addendum D	Employee Behavior
Addendum E	Audit Policy
Addendum F	Wireless Area Networks
Addendum G	Data Integrity
Addendum H	Certification and Accreditation
Addendum I	Universal Serial Bus (USB) Storage Drives/Removable Devices/Media Policy
Addendum J	System Life Cycle Management
Addendum K	Public Key Infrastructure
Addendum L	CSVM Program
Addendum M	Security Education, Training and Awareness
Addendum N	USU Password Policy
Addendum O	Cyber Security Policy Guidance
Addendum P	USU Demilitarized Zone (DMZ) Policy
Addendum Q	Server Security Policy
Addendum R	Acquisition Assessment Policy
Addendum S	Digital Signature Acceptance Policy
Addendum T	Procurement of Desktops and Laptops
Addendum U	Internet and E-Mail Privacy Policy
Addendum V	Visitor Access Control and Common Access Card (CAC) Inspection Program

Governance

1. References.

a. DoDI 8500.01, "Cyber Security ," Certified Current March 14, 2014

b. DoDD 8570.1, "Cyber Security Training, Certification, and Workforce Management," Certified Current April 23, 2007

c. DoDI 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling," May 24, 2011

d. DoD 5200.2-R, "Personnel Security Program," January 1, 1987

2. Purpose and Scope.

The provisions of this document are to establish Cyber Security policy for the Uniformed Services University of the Health Sciences (USU), Bethesda, Maryland.

The term "USU Information System (USU IS)" is used to represent the enclave that defines the accreditation boundary IAW DoDI 8500.01, and is defined to encompass all USU Automated Information System (AIS) Applications, Enclaves, Outsourced Information Technology (IT)-based Processes, and Platform IT Interconnections, such as those supporting e-Business or e-Commerce processes. This includes, but is not limited to; information systems that support special environments, such as the sensors, medical technologies, or utility distribution systems; AIS' under contract to USU; stand-alone AIS' managed by USU; mobile computing devices such as laptops, handhelds, and Android/iOS devices, operating in either wired or wireless mode; and biomedical technologies/devices that may or may not interconnect with a network, but may process and store sensitive information.

The USU Cyber Security Manager provides governance and oversight through the Director, Network Operations and Communications (NOC) and the USU Chief Information Officer (CIO). Governance of the USU Cyber Security Program consists of those functions that contribute to the effective implementation of a USU-wide Cyber Security program and is comprised of the following sub- program elements: program management, planning, budgeting, staffing (human resources), and performance measurement.

3. Responsibilities.

a. CIO shall:

1) Ensure Cyber Security is integrated into all policies and procedures used to plan, procure, develop, implement, and manage the USU IS.

2) Define strategic Cyber Security goals and annual objectives through appropriate Information Management/Information Technology (IM/IT) documents, and ensure such goals and objectives are funded, achieved, and monitored.

3) Collect and report Cyber Security management, financial, and readiness data to meet DoD CIO internal and external reporting requirements.

4) Recommend classification, sensitivity, and need-to-know levels for all USU information and data, and Mission Assurance Category (MAC) Levels for USU all systems.

5) Ensure the USU IS is accredited by the Designated Approving Authority (DAA) in accordance with current DoD Certification and Accreditation (C&A) processes.

6) Establish, resource, and implement a Cyber Security training program for all USU personnel, and a certification program for all USU Cyber Security staff in accordance with DoDD 8570.1.

7) Ensure that Public Key Infrastructure (PKI) implementation within the USU IS complies with DoDI 8520.02.

8) Ensure that the USU IS is assessed for Cyber Security vulnerabilities on a regular basis or when a major change has occurred, and that appropriate Cyber Security solutions to eliminate or otherwise mitigate identified vulnerabilities are implemented.

9) Ensure Cyber Security is integrated into the USU enterprise architecture.

b. Director, Network Operations and Communications shall:

1) Establish a Change Control Board (CCB), a sub-committee of the Automated Information Systems Advisory Committee (AISAC), to ensure all configuration change requests (CCR) are tracked and receive an appropriate disposition. (e.g. approved/implemented or denied with documented reason)

2) Serve as the Chair of the CCB; ensure that CCB meetings are, at a minimum, conducted on a monthly basis; ensure that an agenda is prepared and meeting minutes are kept with an electronic copy in the USU Service Desk Knowledge Documents.

3) Ensure that actions are taken on change requests in a timely fashion by assigning disposition of each CCR, and implementation assignments for approved CCRs.

4) Maintain the USU IS Configuration Management (CM) Plan.

5) Maintain USU IS baseline configurations; to include tracking and maintenance of hardware and software components, such as failed hardware replacement, firmware revisions, patches, and software upgrades.

6) Identify Configuration Items (CI) and document their characteristics.

7) Control and facilitate changes to the characteristics of CI.

8) Perform audits to verify compliance with the USU CM plan.

9) Report to the AISAC Chair the status of all proposed changes, to include relevant discussion items and implementation status of all approved changes.

10) Ensure that USU IS project management documentation is maintained for each IT project through the complete life cycle.

11) Establish a mechanism to receive Software/System Change Requests (SCR) from customers, and ensure they are reviewed for CM implications.

12) Maintain a database of network configuration management baselines as well as software SCR requests and dispositions.

13) Ensure that changes are compliant with system requirements, fit within the USU IS architecture, and that technical integrity and consistency are maintained.

14) Review CCR and SCR reports to resolve implementation questions and priority.

c. Cyber Security Manager shall:

1) Develop and maintain a Cyber Security program that identifies Cyber Security architecture; requirements; objectives and policies; personnel; processes; and procedures.

2) Assess the effectiveness of the USU Cyber Security Program.

3) Develop, staff, and disseminate Cyber Security policy for use by USU.

4) Ensure Risk Assessments are accomplished for all components of the USU IS.

5) Ensure the development and maintenance of C&A documentation by reviewing and endorsing such documentation, and recommending actions to the DAA.

6) Maintain a repository for all C&A documentation and modifications.

7) Budget for C&A security testing, to include travel, risk assessment, documentation review, hardware and software, and specific security training.

8) Ensure that formal incident reporting and response procedures are followed.

9) Ensure that performance measurements are established for the Cyber Security program and are consistent with the Information Management, Technology & Reengineering Performance Objective as reported in the Annual Performance Plan submittal.

10) Provide Cyber Security guidance for the USU enterprise architecture.

11) Provide guidance for security awareness, education, training, and certification.

12) Manage the USU Cyber Security program, to include alert acknowledgements, compliance assessments, and compliance reporting.

13) Staff the Cyber Security function with individuals who, as a team, have the skill mix to manage, execute, and measure the performance of the Cyber Security program.

14) Provide guidance, direction, and oversight on workforce sanctioned policies and procedures to ensure consistent action are taken for failure to comply with security policies for all employees on the workforce.

15) Receive reports of security breaches, coordinate appropriate action to minimize harm, investigate breaches, and make recommendations to management for corrective action.

d. The USU Cyber Security Officer shall:

1) Ensure that all users have the requisite security clearances and supervisory need-to-know authorization, and are aware of their Cyber Security responsibilities, before being granted access to USU IS and connected DoD information systems.

2) In coordination with the Cyber Security Manager, initiate protective or corrective measures when a Cyber Security incident or vulnerability is discovered.

3) Ensure that Cyber Security and Cyber Security-enabled software, hardware, and firmware comply with appropriate security configuration guidelines.

4) Ensure that processes used to recover an information system are monitored, and that all Cyber Security features and procedures are properly restored.

5) Ensure that all information system Cyber Security-related documentation is current and accessible to properly authorized individuals.

6) Implement and enforce all information system Cyber Security policies and procedures, as defined by USU IS C&A documentation.

7) Ensure that information ownership responsibilities are established for each component of the USU IS, to include accountability, access approvals, and special handling requirements.

8) Ensure that all privileged users have obtained or receive the necessary technical and Cyber Security training, education, and certification to carry out their Cyber Security duties.

9) Ensure that compliance monitoring occurs, and review the results of such monitoring.

10) Ensure that Cyber Security inspections, tests, and reviews are coordinated.

11) Ensure that all Cyber Security management review items are tracked and reported.

12) Ensure that incidents are properly reported to the Cyber Security Manager, DAA, and the DoD reporting chain, as required, and that responses to Cyber Security-related alerts are coordinated.

13) Act as a Cyber Security technical advisor to the Cyber Security Manager providing notification of any changes impacting the DoD information system's Cyber Security posture.

e. The Office of Accreditation and Organizational Assessment (Privacy Office) shall:

1) Develop, implement, maintain, and oversee security requirements for electronic Protected Health Information (PHI) and Personally Identifiable Information (PII).

2) Ensure that the requirements for electronic PHI/PII are integrated into all policies and procedures for the planning, procurement, development, implementation, and management of the USU infrastructure and information systems.

3) Ensure a response to alleged violations of rules, regulations, policies, procedures, and codes of conduct by evaluating or recommending the initiation of investigative procedures.

f. The USU Security Manager Shall:

1) Administer the DoD 5200.2-R, "Personnel Security Program," issue guidance or interim authority to access DoD systems, when appropriate, and coordinate letters of trustworthiness for Information Technology/Automated Data Processing (IT/ADP) adjudication packages.

2) Ensure physical security requirements are met for USU buildings and data centers.

4. Revision History.

CHANGE / REVISION RECORD			
Date	**Page/Paragraph**	**Description of Change**	**Made By:**
26 Jan 2011		USU Updates	R. O'Grady
23 May 2014		Review	J. Robertson

SANITIZATION AND DISPOSAL OF ELECTRONIC STORAGE MEDIA POLICY

1. Purpose and Scope.

The provisions of this guide are policy for all USU Components. For USU Contractors, this document is policy, if required by contract; otherwise, it serves as Cyber Security guidance. The USU procedures for sanitization and disposal of electronic storage media and information technology (IT) equipment are implemented to ensure the appropriate actions are executed when disposing of IT equipment and electronic storage media containing Protected Health Information (PHI/PII) and DoD sensitive information (SI), as defined in the Computer Security Act of 1987, Health Insurance Portability and Accountability Act (HIPAA) of 1996, and Privacy Act of 1974. It is pertinent that the Network Operations & Communications (NOC) and Logistics (LOG) comply with the Assistant Secretary of Defense (ASD) Memorandum, "Disposition of Unclassified DoD Computer Hard Drives," June 4, 2001, Federal regulations, and industry's best practices when disposing of USU IT equipment and electronic storage media.

USU IT equipment includes, but is not limited to, hardware (e.g., monitors, keyboards, personal digital assistants, printers, medical technologies), network components (e.g., servers, routers, switches, firewalls), and any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information by USU.

USU defines electronic storage media devices as physical objects that can store electronic data. These devices may include, but are not limited to; computer hard drives, floppy diskettes, magnetic tapes, compact disks (CDs), digital versatile disks (DVDs), and medical devices that store DoD SI and/or PHI/PII. USU Components' electronic storage media that process DoD SI shall be properly sanitized and documented in accordance with this instruction and DoD regulations prior to transferring DoD custody or control, or USU interdepartmental transfers to other entities without having the need-to-know.

This instruction provides NOC and Customer Service Helpdesk personnel (to include contractors) with specific guidance and procedures to ensure disposition and sanitization of USU IT equipment and electronic storage media is executed accordingly prior to transfer within USU or permanent removal from USU and DoD custody.

2. Policy.

It is USU policy that:

a. USU personnel shall adhere to this guidance and procedures to ensure disposition and sanitization of USU IT equipment and electronic storage media is executed accordingly prior to permanent removal from the USU organization.

b. All documents, equipment, and machine-readable media containing sensitive data are cleared and sanitized before being released outside the DoD according to DoDM 5200.1-R, "Information Security Program," dated February 24, 2012 and ASD (C3I) Memorandum, "Disposition of Unclassified DoD Computer Hard Drives," dated June 4, 2001.

c. USU electronic storage media shall be properly sanitized and documented in accordance with this guidance, HIPAA Security Rule, and DoD regulations.

d. The Information Owner shall be designated as the official who is ultimately responsible for establishing appropriate controls for disposal in accordance with DoDI 8500.1 (paragraph E2.1.22).

e. The local Designated Approving Authorities (DAAs) shall approve supplemental instruction to this guidance if further documentation and recording requirements are locally mandated.

f. USU Customer Support Helpdesk and NOC shall utilize the "Record of IT Equipment Sanitization" form (Attachment 1) as the sanitization and clearing label, for ALL dispositions of electronic storage media and USU IT equipment. The signed "Record of IT Equipment Sanitization" label shall be maintained for a minimum of six years to meet HIPAA requirements and to strengthen the USU security posture.

g. Certified overwritten electronic storage media shall be verified on a random basis by two trained individuals other than the person who performed the overwrite process. No fewer than 20% of all overwritten electronic storage media shall be examined in one verification process.

3. Procedures.

a. In accordance with DoD regulations and the HIPAA Security Rule, before a computer system is sold, transferred, or otherwise disposed of, it is necessary to establish procedures for safely managing electronic devices and media. Incorrect disposal of electronic storage media, computers, computer peripherals, and computer software or other IT devices can create the potential of grave information security risks for USU Components. These risks are related to the potential violation of unauthorized release of DoD SI, PHI/PII. Organizations must maintain a record of the movements of hardware and electronic media and any person responsible for those movements. These records must include who has the devices and media, when they had possession, and where they kept the devices or media from the time of original receipt to time of final disposal or transfer to another entity. The mechanism used for recording this information may be manual or automated.

b. To mitigate the potential risk and vulnerabilities, the following procedures must be followed prior to releasing custody or transferring the electronic storage media and IT equipment within the organization to an entity without having the need to access DoD SI, PHI/PII. This procedure also applies to contractor-supplied IT equipment and electronic storage media:

1) Before a computer system is sold, transferred, or otherwise disposed of, all sensitive and/or confidential program or data files on any storage media must be completely erased or otherwise made unreadable in accordance with the ASD (C3I) Memorandum, dated June 4, 2001, "Disposition of Unclassified DoD Computer Hard Drives," and DoD standards (e.g., DoD 5220.22-M).

2) The computer system must be relocated to a designated, continuous physically secured

storage area in accordance with DoDM 5200.1, until sanitization is completed.

3) The term of the license agreement must be complied with whenever software licenses are negotiated with the transfer of equipment or media, or the disposition thereof.

4) Once the sanitization is complete, the process must be certified and the record shall be maintained for a period of six years.

5) Sanitization of Electronic Storage Media and IT Equipment. The following steps outline the acceptable methods to expunge sensitive data from electronic storage media. Sanitization must be performed on electronic storage media and IT equipment to ensure that information is removed from the electronic storage media in a matter that gives assurance that the information cannot be recovered. Before the sanitization process begins, the computer must be disconnected from any network to prevent accidental damage to the network operating system or other files on the network. There are three acceptable DoD methods to be used for the sanitization of electronic storage media and IT equipment:

A. Overwriting.
B. Degaussing.
C. Physical Destruction.

6) The method used for sanitization depends upon the operability of the electronic storage media and IT equipment:

a) Operable electronic storage media and IT equipment that shall be reused must be overwritten prior to disposition. If the operable electronic storage media and IT equipment is to be removed from service completely, it must be physically destroyed or degaussed.

b) If the electronic storage media and IT equipment is inoperable or has reached the end of its useful life, it must be physically destroyed or degaussed. Clearing data (deleting files) removes information from electronic storage media in a manner that renders it unreadable unless special utility software or techniques are used to recover the cleared data. However, because the clearing process does not prevent data from being recovered by technical means, it is not an acceptable method of sanitizing electronic storage media or IT equipment.

7) Overwriting Specifications. Overwriting is an approved method for sanitization of electronic storage media and IT equipment. Overwriting of data means replacing previously stored data on electronic storage media with a predetermined pattern of meaningless information. This effectively renders the data unrecoverable. All software products and applications used for the overwriting process must meet the following specifications:

a) The data must be properly overwritten with a pattern. USU requires overwriting with a pattern, and then its complement, and finally with a random pattern of 1's and 0's (e.g., overwrite first with "00110101," followed by "11001010," then "10010111").

b) Sanitization is not complete until all six passes of the three overwrite cycles are

verified as completed.

c) The software must have the capability to overwrite the entire hard disk drive, independent of any Basic Input/Output System (BIOS) or firmware capacity limitation that the system may have, making it impossible to recover any meaningful data.

d) The software must have the capability to overwrite using a minimum of three cycles (six passes) of data patterns on all sectors, blocks, tracks, and any unused disk space on the entire hard disk medium.

e) The software must have a method to verify that all data has been removed.

f) Sectors not overwritten must be identified.

8) Degaussing Specifications. Degaussing is a process whereby the magnetic media is erased (e.g., returned to a zero state). Hard drives and other electronic storage media seldom can be used after degaussing. The degaussing (demagnetizing) method should only be used when the hard drive and other electronic storage media is inoperable and shall not be used for further service. Please note that extreme care should be used when using degaussers since this equipment can cause extreme damage to nearby telephones, monitors, and other electronic equipment. Also, the use of a degausser does not guarantee that all data on the hard drive will be destroyed. Degaussing efforts should be audited periodically to detect equipment or procedure failures. The following standards and procedures must be followed when hard drives and other electronic storage media are degaussed:

a) Follow the product manufacturer's directions carefully. It is essential to determine the appropriate rate of coercivity for degaussing.

b) Shielding materials (cabinets, mounting brackets), which may interfere with the degausser's magnetic field, must be removed from the hard drive before degaussing.

c) Hard disk platters must be in a horizontal direction during the degaussing process.

d) Degaussing products should be acquired for the National Security Agency's (NSA) Degausser Product List which can be obtained by contacting:

National Security Agency
Attn: S7 Media Technology Center
9800 Savage Road
Ft. George G. Meade, MD 20755-6877
(800) 688-6115 (option 3) or (410) 854-7661

9) Physical Destruction. Electronic storage media and IT equipment must be destroyed when it is defective, cannot be repaired, or cannot be sanitized for reuse. Physical destruction must be accomplished to an extent that precludes any possible further use of the hard drive and

other electronic storage media. This can be attained by removing the electronic storage media and hard drive from the cabinet and removing any steel shielding materials and/or mounting brackets and cutting the electrical connection to the hard drive unit. The hard drive should then be subjected to physical force (pounding with a sledge hammer) or extreme temperatures (incineration) that will disfigure, bend, mangle or otherwise mutilate the hard drive so it cannot be reinserted into a functioning computer.

10) Sanitization of Other Computer Related Storage Media. If there is any risk of disclosure of DoD sensitive data on media other than computer hard drives, the appropriate sanitization methods as outlined in references (d) and (e) must be followed. Particular consideration and attention to detail should be acknowledged when sanitizing floppy disks, tapes, CDs, DVDs, optical disks, etc. Memory components should also be sanitized before disposal or release. Memory components reside on boards, modules, and sub-assemblies. A board can be a module, or may consist of several modules and sub-assemblies.

11) Unlike magnetic media sanitization, clearing may be an acceptable method of sanitizing memory components for release. Memory components are categorized as either volatile or nonvolatile, as described below. Sanitization Procedures should be followed as specified in the table below.

a) Volatile memory components do not retain data after removal of all electrical power sources, and when re-inserted into a similarly configured system do not contain residual data (e.g., Static Random Access Memory (SRAM), Dynamic Random Access Memory (DRAM)).

b) Nonvolatile memory components do retain data when all power sources are discontinued. Nonvolatile memory components include Read Only Memory (ROM), Programmable ROM (PROM), or Erasable PROM (EPROM) and their variants. Memory components that have been programmed at the vendor's commercial manufacturing facility and are considered unalterable in the field may be released; otherwise, DoD Sanitization Procedures must be followed.

Media	**Procedures**
Magnetic Tapes	
Type I*	a, b, or m
Type II**	a or b
Type III***	m
Magnetic Disk	
Bernoullis	m
Floppies	m
Non-Removable Rigid Disk	a, b, d, or m
Removable Rigid Disk	a, b, d, or m

Optical Disk	
Read Many, Write Many	m
Read Only	m, n
Write Once, Read Many (WORM)	m, n

Memory	
Dynamic Random Access Memory (DRAM)	c, g, or m
Electronically Alterable PROM (EAPROM)	j or m
Electronically Erasable PROM (EEPROM)	h or m
Erasable Programmable ROM (EPROM)	l, then c or m
Flash EPROM (FEPROM)	c, then I or m
Programmable ROM (PROM)	m
Magnetic Bubble Memory	a, b, c, or m
Magnetic Core Memory	a, b, c, or m
Magnetic Plated Wire	c and f, or m
Magnetic Resistive Memory	m
Nonvolatile RAM (NOVRAM)	c, g, or m
Read Only Memory (ROM)	m
Static Random Access Memory (SRAM)	c, f, g, or m

*Type 1 magnetic tape includes all tapes with a coercivity factor (amount of electrical force required to reduce the recorded magnetic strength to zero) not exceeding 350 oersteds.

**Type 2 magnetic tape includes all tapes with a coercivity factor between 350 and 750 oersteds.

***Type 3 magnetic tape commonly referred to as high-energy tape (4 or 8mm tape are examples), includes all tapes with a coercivity factor between 750 and 1700.

c) Sanitization Procedure Key:

1. Degauss with a Type I degausser.

2. Degauss with a Type II degausser.

3. Overwrite all addressable locations with a single character.

4. Overwrite all addressable locations with a character, its complement, then a random character and verify. THIS METHOD IS NOT APPROVED FOR SANITIZING MEDIA THAT CONTAINS EXTREMELY CONFIDENTIAL OR SENSITIVE INFORMATION.

5. Overwrite all addressable locations with a character, its complement, and then a random character.

6. Each overwrite must reside in memory for a period longer than the classified data resided.

7. Remove all power to include battery power.

8. Overwrite all locations with a random pattern, all locations with binary zeros, all locations with binary ones.

9. Perform a full chip erase as per manufacturer's data sheets.

10. Perform i. above, then c. above, three times.

11. Perform an ultraviolet erase according to manufacturer's recommendation.

12. Perform k above, but increase time by a factor of three.

13. Destroy – disintegrate, incinerate, pulverize, shred, or melt.

14. Destruction required only if classified information is contained.

d) Certification of Sanitization. Sanitization may be required in instances other than disposal. The University requires their Departments to maintain documentation for all sanitization procedures. The sanitizing process must be documented on an additional form that explicitly outlines the method(s) used to expunge the data from the storage media, the type of equipment/media being sanitized, the name of the individual requesting sanitization, and the name of the person responsible for the sanitization. A form to capture the information shall be utilized to document this process (see Attachment 1).

e) The USU IA Program Office requires that a copy of the proof of sanitization accompany all hard drives earmarked for disposal. This proof may be a copy of the entire "Record of IT Equipment Sanitization" or of Part II of the form. In instances where attaching the paper form to the equipment is not suitable, a label containing the required information may be affixed to the hard drive(s), equipment case (e.g., Central Processing Unit (CPU) box), or appropriate surface. The label must contain the name and signature of the person performing the sanitization, equipment identification and sanitization method used as provided in Part II of the "Record of IT Equipment Sanitization." Equipment Serial and Inventory numbers must match those on the unit inventory.

f) For disposition outside the custody of USU Departments and DoD, an adhesive label shall be affixed to the equipment case to record the sanitization process before transfer. For any remaining questions about leased equipment and equipment maintained through a service agreement, contact the Cyber Security Officer or the Cyber Security Manager.

4. References.

a. DoDI 8500.01, "Cyber Security, March 14, 2014

b. DoDM 5200.1, "Information Security Program," February 24, 2012

c. Public Law 100-235, "Computer Security Act of 1987," January 8, 1988

d. ASD (C3I) Memorandum, "Subject: Disposition of Unclassified DoD Computer Hard Drives," June 4, 2001

e. DoD 5220.22-M, "National Industry Security Program Operating Manual (NISPOM)," January 1995

f. DoD 8580.02-R, DoD Health Information Security Regulation, July 12, 2007

Attachments:
1. USU Record IT Equipment Sanitization Part I
2. USU Record IT Equipment Sanitization Part II

USU RECORD OF IT EQUIPMENT SANITIZATION
PART I

Date Sanitized:
Location of Equipment (include Address, Department & Division):
Person Requesting Sanitization:
Equipment Serial Number:
Equipment Inventory Number:
Equipment Manufacturer/Model:
Equipment/Media Type:
Server Workstation: Assigned to (name of user):
Magnetic Tape (Type I, II or III)
Magnetic Disk (Bernoulli, floppy, non-removable rigid disk, removable rigid disk)
Optical Disk (read many-write many, read only, write once-ready many (WORM)
Memory (DRAM, PROM, EAPROM, EPROM, FEPROM, ROM, SRAM, etc.)
Cathode Ray Tube (CRT) Printer
Other (describe)
Disposition: Transfer Disposal
Return to Contractor
Decommissioning provisions:
Donation
Other (explain)
Repair/maintenance
Equipment/media has been kept in continuous physical protection until sanitization
Information requiring archiving as public records identified and preserved
Temporary backups made (e.g., for equipment scheduled for repair)
Agency asset management procedures completed
Compliant with procedures for disposal of hazardous waste if destroyed
Other (describe)
General description of data residing on equipment/media to be sanitized:

USU RECORD OF IT EQUIPMENT SANITIZATION
PART II

NOTE: This portion of the form must accompany media marked for disposal.

Agency (Cabinet, Department & Division):
Person Performing Sanitization:
Title:
Date Completed:
Equip. Inventory #: Equip. Serial #:
Sanitization Method Used:
DoD-compliant Overwrite (list software used):
Type I Degausser
Type II Degausser
Physical Destruction (disintegrate, incinerate, pulverize, shred, melt)
Other (describe)

Sanitizer Signature: _____

Designated Verification Authority Signature: _____

INCIDENT REPORTING AND RESPONSE PROGRAM

1. Purpose and Scope.

a. The provisions of this guide are policy for all USU departments. For USU Contractors, this document is policy if required by contract; otherwise it serves as Cyber Security guidance.

b. The USU DAA is responsible and accountable for defense of USU networks.

2. Guidance.

a. The term "USU Information System (IS)" encompasses all automated IS applications, enclaves, outsourced IT-based processes, and platform information technology (IT) interconnections as defined in DoDI 8500.01, "Cyber Security," March 14, 2014

b. The terms "computer security incident" and "event reporting" are the notification provided to higher and/or lower echelons regarding out-of-the-ordinary events such as a loss of data integrity, a denial of system resources, the penetration of a system's defenses either by an insider or an outsider, the misuse of legitimate computer resources, or the actual damage to information or resources. A computer security incident may lead to the breach of Personally Identifiable Information (PII)/Protected Health Information (PHI). Breach reporting is managed by the Office of Accreditation and Organizational Assessment (Privacy Office).

c. This policy provides guidance for incident handling within USU. Any event with the potential to adversely affect an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service is a threat. Such events should be considered computer security incidents.

d. Computer security incidents are caused by policy and procedure violations, as well as outside intrusions and the exploitation of system vulnerabilities. These events could result in loss of data integrity, denial of system resources, penetration of a system's defenses either by an insider or an outsider, misuse of legitimate computer resources, or damage to information or resources.

e. An effective response to computer security incidents requires prompt recognition of the problem and immediate mobilization of a skilled staff. Prior documentation of procedures and clear delegation of responsibilities are necessary when responding to any computer security incident. Essential components of a computer incident response are the elimination of points of vulnerability and the application of lessons learned.

f. The Verizon Security Operations Center (VSOC) is the Computer Network Defense Service Provider (CNDSP) for the USU.edu network.

g. For incident reporting purposes, the USU enclave includes the network located on the USU main campus and buildings on the NSA Bethesda and extended to the Twinbrook, Rockledge, Rockville Pike, San Antonio, and Forest Glenn off-site locations.

3. Procedures.

a. Any user noticing anomalous or suspicious activity (incident or reportable event) must report the situation immediately to the Customer Service (CSD) Helpdesk. The CSD Helpdesk will report the activity to the USU Cyber Security Branch and the Network Operations and Communication (NOC) Manager.

b. The Chief, Cyber Security Branch and Network Operations Manager will report incidents or events affecting networks directly to the CNDSP. The CNDSP will report to DoD. The required reporting times (Appendix B) must be met.

c. The USU Cyber Security Branch will report changes in the status of events, incidents, and incident- handling actions. The USU Cyber Security Branch will report these status updates to the CNDSP and to the Office of Accreditation and Organizational Assessment (Privacy Office) when:

1) Incidents involve Health Insurance Portability and Accountability Act (HIPAA)/ Protected Health Information (PHI)/Personally Identifiable Information (PII).

2) There are increases, decreases, or changes in the nature of the reportable event or incident activity.

3) Corrective actions are taken that change the status of the reportable event or incident activity.

4) A reportable event or incident has been declared closed.

Updates must be reported to the CNDSP every 24 hours, until an incident is closed. The CNDSP will forward updates to CYBERCOM.

d. In the event an attack is detected by the VSOC and reported to USU, the Chief, Cyber Security Branch will coordinate internal notification and follow-on responses.

e. The Chief, Cyber Security Branch shall ensure that incidents are properly reported to the Designated Accrediting Authority (DAA), and USU CIO. The Cyber Security Branch will ensure effective incident management in accordance with reference *(h)*.

f. An event or set of events might result in an incident reported in the Joint Computer Emergency Response Team (CERT) Database. Once verified, incidents are reported and updates are provided with enough granularity for analysis to determine corrective action and threats to DoD operations.

g. Reportable incidents/events must be labeled according to categories in Appendix A.

h. Threshold reporting times, according to MAC, and reporting notification methods for unclassified systems are outlined in Appendix B, Attachment 2.

i. An incident may need the involvement of law enforcement. If the Chief, Cyber Security Branch, in consultation with the Network Operations Manager, suspects criminal activity, especially for Categories 1-4, 7, and 9 incidents (Appendix A), he or she must contact applicable law enforcement organizations. In rare circumstances, an incident requires reporting to counterintelligence. Prior to taking such action, the Chief, Cyber Security Branch and the Network Operations Manager will notify both the USU General Counsel and the USU DAA through the Office of the CIO. Chief, Cyber Security Branch and the Network Operations Manager will notify the CNDSP and the USU Office of Accreditation and Organizational Assessment (Privacy Office) (when incidents involve HIPAA/PHI/PII), when they make the decision to contact law enforcement and/or counterintelligence. At USU, all suspected criminal activity-related incidents are first reported to the Naval Support Activity - Bethesda (NSAB) Base Police. The NSAB Base Police serve as the first responders and would conduct the preliminary investigation/recovery of materials, etc. Subsequently, the NSAB Base Police would determine if an incident warrants higher level reporting/investigation. If such a determination is made, then the Naval Criminal Investigative Service (NCIS) would be the next higher level of law enforcement agency contacted. Contact information for the primary law enforcement agency is as follows: NSAB Base Police at 301-295-1246.

j. The following computer security incident response procedures are provided as baseline requirements for incident management:

1) Detection - If a system user or administrator discovers suspicious activity, he or she must report it to the CSD Helpdesk. Network administrators will notify the Network Operations Manager and Chief, Cyber Security Branch. The Chief, Cyber Security Branch and the Network Operations Manager will assess the event and label it as either a "reportable event" or confirmed incident:

a) A reportable event is any occurrence, not yet assessed, that may affect the performance of an information system.

b) A confirmed incident is any information system-assessed occurrence resulting in actual or potentially adverse effects on an information system.

c) The Chief, Cyber Security Branch and the Network Operations Manager also will assign reportable events or confirmed incidents to one of the categories (re-categorize, if applicable) from Appendix A.

2) Documentation - The Chief, Cyber Security Branch and Network Operations Manager will document the potential incident and all actions taken for resolution of the incident.

3) Containment - The Network Operations Manager, in consultation with the Chief, Cyber Security Branch and CNDSP, will take all necessary mitigating actions to contain the incident.

4) Initial Reporting - The Network Operations Manager, Chief, Cyber Security Branch, and the USU Office of Accreditation and Organizational Assessment (Privacy Office) (when

incidents involve HIPAA/PHI/PII), will submit an initial report to the CNDSP and CYBERCOM. Reporting timelines will vary according to activity category and system MAC (Appendix B). In the event the incident involves PII, it must be reported to the United States Computer Readiness Team (US CERT) within 1 hour, the Office of the Secretary of Defense and Joint Staff (OSD/JS) within 24 hours, and the Defense Privacy Office within 48 hours.

5) Analysis - The Network Operations Manager will collect all data about the incident including the following:

a) Logs.

b) Personal accounts.

c) Inventory of the systems.

The Network Operations Manager will validate circumstances surrounding the incident by confirming the following data points:

a) Type.

b) Intrusion method used.

c) Vulnerabilities.

6) Determination - The Network Operations Manager, CNDSP, and the Chief, Cyber Security Branch will determine both the Operational Impact (OI) and Technical Impact (TI) of the incident.

7) Coordination - The Director, MHS Cyber Security Program Office will coordinate with other agencies and components as necessary.

8) Develop COAs - The Network Operations Manager, in consultation with the CNDSP, will develop Courses of Action (COAs).

9) Submit Follow-on Reports - The Network Operations Manager will submit updated information on the incident to the CNDSP. Absent direction to the contrary, submitted reports are due within eight hours of new data.

10) Recover from Incident - The Network Operations Manager, in consultation with the CNDSP, will fully restore data and systems and execute the necessary changes to network configuration.

11) Submit Final Documentation - The Chief, Cyber Security Branch and Network Operations Manager will submit final reports (including impact assessments) within 24 hours of the incident's resolution.

k. Following a systemic event or as a precursor to accreditation, information owners may request a baseline review, known as a Vulnerability Assessment Activity (VAA), of its enclaves and network systems.

l) Requests for such resources must follow a specific chain of authority.

a) The CIO will notify the DAA regarding the need for a baseline review.

b) The DAA must formally request that the CNDSP begin a VAA.

c) These reviews will follow three phases:

Phase I – A Vulnerability Assessment Team (VAT) will examine information systems, networks, workstations, and Cyber Security policies to determine the adequacy of existing security measures and identify security deficiencies.

Phase II – Once the VAT has identified vulnerabilities, the "Blue Team" will provide guidance on areas of concern. The team will function as a "friendly assist" to expeditiously remedy deficiencies and enhance policy and procedures.

Phase III – After the VAT and Blue Team (a team of knowledgeable personnel normally formed by DISA to assist in vulnerability mitigation) have addressed all deficiencies, the "Red Team" (A team of personnel knowledgeable in adversaries' and offensive attacks) attacks the USU IT infrastructure and attempts to discover additional weaknesses and vulnerabilities. These teams will work closely with system / network owners to demonstrate how future attacks might occur. Team leaders also will submit to system/network owner's recommendations for protecting their systems.

4. References.

a. Health Insurance Portability and Accountability Act of 1996

b. DoDD 8500.01, "Cyber Security," Certified Current March 14, 2014

d. DoD Chief Information Officer (CIO) Memorandum, "Department of Defense (DoD) Guidance on Protecting Personally Identifiable Information (PII)," August 18, 2006

e. CJCSM 6510.01, "Defense-in-Depth: Cyber Security and Computer Network Defense (CND)," March 25, 2003

f. CJCSI 6510.01E, "Cyber Security and Computer Network Defense,"March 8, 2006 (with changes through 14 March 2007)

h. Joint Task Force Global Network Operations (JTF-GNO) Communications Tasking Order (CTO) 05-13, "Directive for Interim Guidance for Incident Handling Program," GENADMIN MSGID 231703Z Sept 05

5. Revision History.

CHANGE / REVISION RECORD			
Date	**Page/Paragraph**	**Description of Change**	**Made By:**
May 2014		Annual Review	cjodrie

Attachments:
1. Appendix A
2. Appendix B
3. Appendix C

Appendix A

Category	Description
1	**Root Level Intrusion (Incident):** Unauthorized privileged access (administrative or root access) to a DoD system.
2	**User Level Intrusion (Incident):** Unauthorized non-privileged access (user level permissions) to a DoD system. Automated tools, targeted exploits, or self- propagating malicious logic may also attain these privileges.
3	**Unsuccessful Activity Attempt (Event)**:** Attempt to gain unauthorized access to the system, which is defeated by normal defensive mechanisms. Attempt fails to gain access to the system (i.e. attacker attempt valid or potentially valid username and password combinations) and the activity cannot be characterized as exploratory scanning. Can include reporting of quarantined malicious code.
4	**Denial of Service (Incident):** Activity that impairs, impedes, or halts normal functionality of a system or network.
5	**Non-Compliance Activity (Event):** This category is used for activity that due to DoD actions (either configuration or usage) makes DoD systems potentially vulnerable (e.g., missing security patches, connections across security domains, installation of vulnerable applications, etc). In all cases, this category is not used if an actual compromise has occurred. Information that fits this category is the result of non-compliant or improper configuration changes or handling by authorized users.
6	**Reconnaissance (Event):** An activity (scan/probe) that seeks to identify a computer, an open port, an open service, or any combination for later exploit. This activity does not directly result in a compromise.
7	**Malicious Logic (Incident):** Installation of malicious software (e.g., Trojan, backdoor, virus, or worm).
8	**Investigating (Event):** Events that are potentially malicious or anomalous activity deemed suspicious and warrants, or is undergoing, further review. No event will be closed out as a category 8. Category 8 will be re-categorized to appropriate Category 1-7 prior to closure.
9	**Explained Anomaly / Activity (Event):** Events that are initially suspected as being malicious but after investigation are determined not to fit the criteria for any of the other categories (e.g., social engineering).

** Event - Any occurrence, not yet assessed, that may affect the performance of an information system. (CJCSI 6510.01E, reference (i))

Appendix B

Category and Title	Requirement
1) Root Level Intrusion	MAC II — Discovery / Awareness: – Telephone: 15 mins — Follow-up Report: – E-mail: Appendix C format 4 hours — Update report: – E-mail: Appendix C format every 24 hours until close of incident MAC III — Discovery / Awareness: – Telephone: 2 Hours — Follow-up Report: – E-mail: Appendix C format 4 hours
2) User Level Intrusion	MAC II — Discovery / Awareness: – Telephone: 15 mins — Follow-up Report: – E-mail: Appendix C format 4 hours — Update Report: – E-mail: Appendix C format every 24 hours until close of incident MAC III — Discovery / Awareness: – Telephone: 2 Hours — Follow-up Report: – E-mail: Appendix C format 4 hours

Category and Title	Requirement
3) Unsuccessful Activity Attempt	MAC II – Discovery / Awareness: – Telephone: 15 mins – Follow-up Report: – Appendix C format 24 hours following CNDSP validation MAC III – Discovery / Awareness: – Telephone: 4 Hours – Follow-up Report: – E-mail: Appendix C format 24 hours following Discovery / Awareness
4) Denial of Service	MAC II – Discovery / Awareness: – Telephone: 15 mins – Follow-up Report: – Appendix C format 4 hours following Discovery / Awareness – Update Report: – E-mail: Appendix C format every 24 hours until close of incident MAC III – Discovery / Awareness: – Telephone: 4 Hours – Follow-up Report: – E-mail: Appendix C format 12 hours following Discovery / Awareness

Category and Title	Requirement
5) Non-compliance Event	MAC II — Discovery / Awareness: – Telephone: 4 hours for severe attack, 12 hours for moderate — Follow-up Report: – Appendix C format 4 hours following for severe attack, 72 hours for moderate MAC III — Discovery / Awareness: – Telephone: 2 hours — Follow-up Report: – Appendix C format 24 hours following Discovery / Awareness
6) Reconnaissance Event	MAC II — Discovery / Awareness: – Telephone: 15 mins — Follow-up Report: – Appendix C format 12 hours following Discovery / Awareness MAC III (Low Level Attacks) — Discovery / Awareness: – Telephone: 2 hours — Follow-up Report: – Appendix C format 24 hours following Discovery / Awareness

Category and Title	Requirement
7) Malicious Logic	MAC II — Discovery / Awareness: – Telephone: 15 mins, 2 hours for a moderate attack — Follow-up Report: – E-mail: Appendix C format w/in 4 hours, 8 hours for a moderate attack — Update Report: – E-mail: Appendix C format every 24 hours until close of incident MAC III (Low Level Attacks) — Discovery / Awareness: – Telephone: 2 hours — Follow-up Report: – Appendix C format 24 hours following Discovery / Awareness
8) Investigating (Event)/ Unknown	MAC II — Discovery / Awareness: – Telephone: Immediately, follow-up call by asset owner 2 hours — Follow-up Report: – E-mail: Appendix C format consistent with most severe interpretation (See above) — Update Report: – E-mail: Appendix C format consistent with most severe interpretation (See above) MAC III (Low Level Attacks) — Discovery / Awareness: – Telephone: 2 hours — Follow-up Report: – Appendix C format 24 hours following Discovery / Awareness (Report every 24 hours until assigned to category 1-7.)

Category and Title	Requirement
9) Explained Anomaly/ Activity (Event)	MAC II — Discovery / Awareness: – Telephone: As soon as practical MAC III (Low Level Attacks) — Discovery / Awareness: – Telephone: 2 hours — Follow-up Report: – 24 hours following Discovery / Awareness

Appendix C
Cyber Security Computer Incident Reporting Form

Field	Description
CERT/CIRT (Computer Incident Response Team) Incident	Identify the reporting CERT/CIRT's reference number for tracking the incident.
Primary Incident Category	Identify access level gained as per Appendix A
Secondary Incident Category	Identify any sub access level gained, if more than one category applies, as per Appendix A.
Attack Vector	Identify attack vector.
Weakness	Identify system weakness.
Last Update	ZULU date time group (DTG)(DTG Example: 141615Z AUG 06) of the last time the report was updated. Provide Year/Month/Day/Hour/Minute /Seconds.
Incident Start Date	ZULU DTG of the earliest event that was incorporated into the incident. Provide Year/Month/Day/Hour/Minute /Seconds.
End Date	ZULU DTG that incident actually ended. Provide Year/Month/Day/Hour/Minute
Status	Status of the incident ("OPEN" or "CLOSED").
System Classification	Classification of the system under attack. "UNCLASSIFIED", "CONFIDENTIAL", "SECRET", "TOP
Detecting Unit or Organization	Name of reporting Unit or Organization.
Affected Unit or Organization	Name of reporting affected Unit or Organization.
Action Taken	Indicates what action has been taken in response to the incident. Include notifications and associated reports. Include whether a copy of a medium was taken (image hard drives, or logs collected and disposition of mediums and logs).
Organization Tracking	Uniformed Services University of the Health Sciences (USU)
CERT Date Reported	ZULU DTG of when the incident was first reported to the CNDSP / CYBERCOM. Provide Year/Month/Day/Hour/Minute /Seconds.
Operational Impact	Identify any detrimental effects on ability to perform mission.
Major Command	Defense Health Agency (DHA).
System Impact	This is a subjective field, but it is critical to get a general sense of the impact on operations of an incident.
Systems Affected	Number of systems affected by the incident.
Staff Hours Lost	This is reported as an update record and may cause the Impact field to be updated. Amount of time your technical support required to identify, isolate, mitigate, resolve and recover from the attack and repair the attacked system (do not include analyst time spent analyzing the incident).
Exercise Name	Name of the exercise, if applicable.
Event Description	Provide a detailed description of the event, including what happened, how it occurred and the current action taken to mitigate
Source IP (Internet Protocol) and Port	Provide source IP with resolution data identifying owner and country of source IP machine. If the intruder is known, provide all identifying information to include objective of intruder, if known. (Source IP is not necessarily indicative of true origin). Footnote the source of resolution/attribution data – i.e., ARIN.org.

Field	Description
Intruder(s) (if known)	Identify the intruder or group that is responsible for the incident, if known.
Origin (country) (if known)	Identify the Source IPs country of origin.
Target IP(s) and Port	Provide target IP with resolution identifying responsible command and physical location of target IP machine. Footnote the source of resolution/attribution data – i.e. DoD NIC, NSLOOKUP, WHOIS. If machine is behind a NAT'ed (network address translation enabled) router or firewall then also provide the wide area network (WAN) routable address (i.e. the Internet/Secret Internet Protocol Router Network (SIPRNET) routable IP address).
Technical Details	Provide a narrative description of the incident with technical details. Include DTGs of significant events (start, stop, or change of activity). State the use of the targeted system and whether the system is online or off-line. Indicate whether the incident is ongoing.
Physical Location (base, camp, post or station)	Identify the facility that is affected by the intrusion and/or owns the Target IP and where the physical system resides: USU Main Campus on NSAB Twinbrook Rockledge SIMCEN (Forest Glenn Annex)
Technique, tool or exploit used	Identify the technique, tool, or exploit that was used to exploit the vulnerability.
Operating System (OS) and version of OS	Record the operating system and version number of the operating system where the incident occurred.
Use of target (e.g., web server, file server, host)	If applicable, for what the intruder/attacker used the target system for after it was exploited, if applicable.
DoD Network	Identifies network on which the incident occurred: NIPR
Comments	Provide any amplifying information about the incident.
Synopsis	Provide an executive summary of the incident.
Contact Information:	Name:
	Organization:
	Telephone:
	Fax:
	E-mail:

EMPLOYEE BEHAVIOR POLICY

1. Purpose.

The provisions of this guide are policy for all USU Components. For USU Contractors, this document is policy if required by contract; otherwise it serves as Cyber Security guidance. This implementation guide provides the rules and policies governing the behavior of USU Components who manage, design, develop, operate, access DoD ISs, or access DoD data, while accessing or using DoD resources (e.g., USU network, internet, e-mail, and electronic devices connected to the USU network).

a. DoD 5500.7-R, "Joint Ethics Regulation (JER)," (Changes 1-4), dated August 1993, Section 2-301, directs that the use of Federal government resources, including personnel, equipment, and property (e.g., computers, electronic mail, and Internet systems), "shall be for official use and authorized purposes only." "Official use" refers to uses that directly further the interests of the DoD and the duties prescribed for the individual position. "Authorized purposes" refers to personal use within specified limits as permitted by an appropriate level supervisor. The specified limits are described below:

1) Does not adversely affect performance of official duties.

2) Is of reasonable duration and frequency.

3) Whenever possible, is made during the member's personal time (before/after duty hours, during lunch, or authorized breaks).

4) Serves a legitimate DoD interest.

5) Does not reflect adversely on DoD or USU.

6) Does not overburden the communications system.

7) Results in no significant additional cost to DoD or USU.

2. Scope.

This policy applies to all USU users to include faculty, staff, students, guests, contractors and volunteers that utilize USU IS resources.

3. Policy.

a. Authorized Purposes. The USU Employee Behavior Policy is established for limited personal use of DoD resources consistent with the above-listed limitations. Limited personal use would include the following activities (e-mail or web based).

1) E-mailing short messages to a relative or colleague.

2) Receiving e-mail (as long as comparable receipt would be acceptable via telephone, and

is no more disruptive than a telephone call).

3) Announcing USU-related activities (e.g., office luncheons, retirement or departure events, and holiday office parties).

4) Making a medical, dental, auto repair, or similar appointment.

5) Accessing the internet for professional development purpose.

6) Checking investment status (e.g., stock prices) or authorizing a financial transaction.

7) Reading a news or business magazine.

b. Use Limits. In order to ensure that such authorized personal use does not adversely affect the performance of official duties, personnel may only go online when needed and must immediately disconnect (close their browser) when they are finished. Users must terminate and logoff the network on completion of their business in order to share network resources in multi-user environments and prevent unauthorized access. Remote dial-in access may only be used for official use (e.g., mission-related dial-in from home or temporary duty (TDY) location). Personal use of the network dial-in capability is prohibited.

c. Workstation Position. In order to protect sensitive information (SI) during the performance of official duties, users must position monitors so that casual passersby cannot view the screen.

d. Authentication. System users will utilize the Common Access Card (CAC) to access the USU IS. Users that are not eligible to acquire a CAC or Volunteer Logical Access Credentials (VOLAC), will be identified as non- CAC users in the Active Directory and will be issued a username and 15 character password. Attempts to circumvent authentication measures constitute a violation of USU and DoD policy.

e. Software License. System users, who illegally acquire and/or use unauthorized unlicensed copies of software, shall be held accountable under U.S. copyright law. Violations might result in civil/criminal penalties and employee termination.

f. Modification. System users are restricted from adding or removing devices or hardware from USU ISs.

g. Off-site Computing. Remote access is reserved for performance of official duty only (e.g., mission-related Virtual Private Network (VPN) access from home or travel). Personal use of the network VPN capability is prohibited. Only Government furnished equipment (GFE) and Henry M. Jackson Foundation authorized equipment (e.g. assigned laptops) may be used to remotely access the USU network.

h. Removal of Sensitive Data. No sensitive data (including Protected Health Information (PHI) or Personally Identifiable Information (PII) may be removed without the Designated Accrediting Authority (DAA) approval.

i. Personally Identifiable Information (PII). USU ISs containing DoD data identified as PII shall be categorized on one of the two categories:

1) High Impact – A compilation of 500 or more electronic records containing PII stored on a single device, accessible through an application or service. A compilation of 500 or less electronic records whereby the information owner requires additional protection measures.

2) Moderate Impact – Any PII electronic records containing PII not identified as High impact.

j. High Impact PII records shall not be routinely processed or stored on mobile computing devices or removable media without express written approval of the DAA.

k. Any mobile computing device containing High Impact PII removed from the protected workplace, including those approved for routine processing, shall:

1) Be signed in and out with a supervising official designated in writing.

2) Require DoD-approved PKI certification to be accessed.

3) Enable screen-lock functionality within 15 minutes of workstation inactivity.

4) Require full disk encryption utilizing the USU McAfee Endpoint Encryption.

l. Encryption of Sensitive Data. Encryption of data for transmission and storage from mobile/wireless devices is required. Authorized Users of mobile/wireless devices are required to ensure all sensitive information (e.g. Privacy, Patient Health Information (PHI/PII)) is encrypted, whether data is in transit or stored at rest. Encryption is required regardless of storage media type. Types include, but are not limited to; Portable Electronic Devices (PEDs), Personal Digital Assistants (PDAs), cell phones, flash drives, memory sticks, zip and compact disks, removable disk drives, and laptop computers.

4. Procedures.

a. Unauthorized Purposes. The following list provides examples (not all-inclusive) of uses that would be unauthorized and inconsistent with the appropriate use of Federal government resources:

1) Use for commercial purposes.

2) Soliciting business, advertising, or engaging in other selling activities in support of private business enterprises or outside employment.

3) Fundraising activities.

4) Use of a DoD network as a staging ground or platform to gain unauthorized access to other systems.

5) Creating, copying, or transmitting chain letters or other unauthorized mailings regardless of the subject matter.

6) Accessing, creating, downloading, viewing, storing, copying, or transmitting sexually oriented or racist materials.

7) Accessing, creating, downloading, viewing, storing, copying, or transmitting materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited.

8) Endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity.

9) Posting USU information to external newsgroups, bulletin boards, or other public forums without authority.

10) Accessing sites known for hacker attacks or hacker activity.

11) Downloading shareware/freeware software or executable programs (e.g., .EXE, .COM, .BAT, or script.INI files).

12) Accessing or participating in Internet Relay Chat (IRC) sessions, which is an application layer protocol that facilitates transfer of messages in the form of text.

13) Participating in "spamming;" that is, exploiting list servers or similar group broadcast systems for purposes beyond their intended scope to provide widespread distribution of unsolicited e-mail.

14) Participating in "letter-bombing;" that is, sending the same e-mail repeatedly to one or more recipients to interfere with the recipient's use of e-mail.

15) Opening e-mail attachments from unknown or questionable sources or opening attachments from such sources without downloading to disk and virus scanning.

16) Attempting to circumvent, disable, or compromise USU Component security and authentication measures.

17) Sending, whether initiating or replying to, inappropriate messages or messages containing inappropriate language.

18) Transmitting SI or Protected Health Information via the internet without appropriate security controls (e.g., encryption) in place.

b. Consent to Monitoring. Use of DoD resources and equipment is neither private nor anonymous. In accordance with laws and regulations, the use of such resources may be

monitored. Any use of DoD resources and equipment serves as consent to monitor and record any type of use – official or personal, authorized or unauthorized. Personnel using DoD resources receive training on Security Guidelines and are required to acknowledge their responsibilities. Personnel should remember that electronic transmissions can create a permanent record of the information transmitted. Thus, even if the parties intend the activity to be a temporary transfer of information, the system may be maintaining a permanent record of the message.

c. Sanctions for Misuse. The limited personal use of USU resources is a privilege and does not create a right to use those resources for non-USU purposes. Unauthorized or improper use of USU communications resources could result in limitations on or loss of use of such resources, disciplinary or adverse actions (including criminal penalties and revocation of access to SI), or personnel being held financially liable for the cost of improper use.

5. Responsibilities.

a. As necessary, the Cyber Security Officer may use software to monitor the use of the USU resources, as deemed appropriate, to include e-mail, and shall notify senior management of any unauthorized activity, misuse, or abuse.

b. The Cyber Security Officer shall ensure information owners assign impact categories for PII records.

c. The Cyber Security Officer shall ensure supervisors establish logging and tracking procedures for PII removed from the protected work place.

d. The USU CIO shall enforce compliance with all restrictions on the use of DoD resources. Compliance shall be enforced through a variety of means including:

1) Administrative sanctions specifically related to the system (e.g., loss of system privileges).

2) General sanctions as are imposed for violating other rules of conduct regarding system use.

3) Civil and criminal penalties.

e. As a requirement for network access, users shall be required to sign a User Agreement that outlines:

1) User responsibilities.

2) Potential sanctions for non-compliance with established rules.

f. Laptops assigned to users who most likely require remote access, must only be accessible by CAC.

g. Supervisors must submit written approval to Cyber Security Officer's before allowing users to remove sensitive data (including PHI/PII) from USU facilities. The submitted approval must specify date, type of data, reason for being removed from the facility, and identifying data from the user's assigned laptop.

1) Users must sign a Data Use Agreement (DUA) acknowledging that they are responsible for maintaining the physical security and confidentiality of sensitive information.

2) Users shall be required to sign a User Agreement that outlines their responsibilities. Non-compliance with established rules shall result in the suspension of the user's account privileges.

3) Users are required to comply with the parameters of this policy and to report misuse to their supervisors. Users are reminded to apply the same standards governing use of the USU Network to the use of any DoD resource regardless of location (i.e., TDY or other government sites). Questions regarding "authorized purposes" or "use limits" should be directed to the supervisor who shall forward them to the Cyber Security Officer for action.

4) A set of rules that describe the Cyber Security operations of the USU Components, and clearly delineate the Cyber Security responsibilities and expected behavior of the user shall be in place. The rules shall include the consequences of inconsistent behavior or non-compliance. A signed acknowledgement of the USU Cyber Security Rules of Behavior shall be a condition of access to a USU system.

6. References.

a. DoD 5500.7-R, "Joint Ethics Regulation (JER)," August, 1993 (Changes 1-4)

b. DoDD 5500.7, "Standards of Conduct," August 30, 1993

c. DoDI 8500.01, "Cyber Security" March 14, 2014

d. Public Law 104-191, "Health Insurance Portability and Accountability Act of 1996," August 21, 1996

e. H.R. 20, 101st Congress, Hatch Act Reform Amendments of 1990

7. Revision History.

CHANGE / REVISION RECORD			
Date	**Page/Paragraph**	**Description of Change**	**Made By:**

AUDIT POLICY

CHANGE LOG

This record shall be maintained throughout the life of the document. From the initial creation of the document each published update shall be recorded. A revision shall be made whenever the cumulative changes reach ten percent (10%) of this document's content. A Review of documents are made annually or earlier when needed.

CHANGE / REVISION RECORD			
Date	**Page/Paragraph**	**Description of Change**	**Made By:**
2009		Initial Document	R. O'Grady
Jan 2011		Format for USU	
May 2014		Annual Review	jrobertson

CYBER SECURITY CONTROL MATRIX

The following table lists the DIACAP Cyber Security Controls that are satisfied through this artifact. Click on the hyperlink located under the box heading "Section Cross Reference" to go to the appropriate paragraph.

IA Control Number	IA Control Name	Section Cross Reference
	DoDI 8500.01	
DCCT-1	Compliance Testing	Para_5_2
DCFA-1	**Access Control** - Processes and Procedures	Para_1_1
DCSP-1	**Access Control** - Control of access to and integrity of hardware, software, and firmware that perform security functions.	Para_3_9
EBRP-1	Remote Access Audit Log Reviews	Para_4_5
EBRU-1	Remote Access Information Protection	
ECAD-1	**Access Control** - Access to Need-to Know	Para_3_3
ECAN-1	**Access Control** - Access to Need-to Know-Discretionary Access Control.	Para_3_3
ECCD-1, ECCD-2	**Access Control** - Transaction Recording - Access Control Mechanisms exist.	Para_3_8
ECAR- 1 ECAR-	Audit Record Content – Public Systems Audit Record Content – Sensitive Systems Audit Record Content – Classified	Para_4_3
ECAT-1, ECAT-2	Audit Trail, Monitoring, Analysis and Reporting	Para_3_3 & Para_4_6_c
ECLO-1	**Access Control** - Logon and Multiple Logon controls for access.	Para_3_3_b
ECLP-1	**Access Control** - Privileged User Accounts	Para_3_4
ECMT-1, ECMT-2	Conformance Monitoring and Testing	
ECPA-1	**Access Control** - All privileged user accounts are established and administered in accordance with a role- based access scheme.	Para_3_5
ECRG-1	Audit Reduction and Report Generation	Para_4_6
EBRP-1	Remote Access Audit Log Reviews	Para_4_5
ECRR-1	Audit Record Retention	Para_4_7_3
ECTB-1	Audit Trail Backup	Para_4_9
ECTP-1	Audit Trail Protection	Para_4_4
PRNK-1	**Access Control**-Need to Know - ensure only valid need-to- know have access.	Para_3_3
IAAC-1	**Access Control** - A comprehensive account management process is implemented to ensure that only authorized users can gain access to workstations, applications, and	Para_3_3
IAGA-1	**Access Control**-Group authenticators for application or network access may be used only in conjunction with an individual authentication.	Para_3_6
IAIA-1	**Access Control - Group** the system requires users to provide unique user identifier in the form of a unique token or user ID and password before accessing the system either initially or after a screen lock program is	Para_3_0
IATS-2	**Access Control** - Identification and authentication is accomplished using the DoD PKI Class 3 or 4	Para_3_7

Table of Contents

EXECUTIVE SUMMARY

In the past, the Department of Defense (DoD) has been the victim of successful hackers that were able to penetrate DoD computers before they were detected or identified. Many DoD internet sites have also been blocked by coordinated "denial-of-service" attacks. All organizations must also cope with the threat of hacking from individuals within the organization.

This document has been prepared as the policy of the Uniformed Services University of Health Sciences (USU), Network Operations and Communications (NOC) regarding system and incident auditing. The audit policy has been developed to enhance the confidentiality, integrity, and availability of sensitive DoD Information Systems (IS) and will assist USU personnel with Cyber Security audit information to meet the requirements, standards, controls, and options that must be in place for secure network operations.

Procedures include responsibilities, a plan to assess, train for, monitor, and conduct audit procedures within the NOC in the defense of the system and connected DoD computer networks.

AUDIT POLICY

1. INTRODUCTION

1.1 Purpose

The audit policy has been developed to enhance the confidentiality, integrity, and availability of sensitive DoD Information Systems and will assist USU personnel with Cyber Security audit information to meet the requirements, standards, controls, and options that must be in place for secure network operations.

This audit policy presents information and procedures regarding security audits and Cyber Security scanning to be performed by NOC personnel, to include the Cyber Security Manager, the Cyber Security Officer, and all Network Administrators (NA) and System Administrators (SA).

a. NOC personnel shall use the following approved tools to perform audits of the USU.

1) Splunk Audit Monitoring Tool.

2) eEye Retina Vulnerability Scanning Tool.

3) DoD Security Readiness Review (SRR).

b. Audits will be conducted to:

1) Check the integrity, confidentiality and availability of information and resources.

2) Investigate possible security incidents.

3) Ensure conformance to NOC security policies.

4) Monitor user or system activity, where appropriate.

1.2 Background

Security is a large concern for the DoD (i.e., the warfighter), and a comprehensive audit program will assist in decreasing the vulnerability of DoD sensitive information. The USU will monitor its systems for possible unauthorized intrusion and other attacks as part of the daily routine/duties of NOC Cyber Security personnel.

1.3 Overview

Auditing is the independent review of records and activities to assess the adequacy of system functionality and security. The review process is used to check that compliance with established policy and operational procedures, to verify that the security of the system has not been breached, and to recommend necessary changes in controls, policy, or procedures.

1.4 Scope

This policy covers all components of the USU IS, regardless of where they are installed. This policy also covers all computer and communications devices that are on the USU IS. Audits will not include Denial of Service checking activities.

2. RESPONSIBILITIES

2.1 The Information Systems Security (ISSM)

The Designated Approving Authority (DAA) shall appoint the Cyber Security Manager in writing. The Cyber Security Manager's main function is to develop and enforce a formal Cyber Security training program. The Cyber Security Manager also assists the Chief Information Officer (CIO) to identify and validate Cyber Security resource requirements, provides input to the Configuration Control Board (CCB) for configuration management controls, serves as a voting member of the CCB, and ensures that NOC personnel and Server Administrators (SAs) are performing security audits to validate conformance to security policies and procedures.

2.2 Information Systems Security (ISSM)

The CIO shall appoint the Cyber Security Manager in writing. The main duties of the Cyber Security Manager are to enforce Cyber Security policy, guidance, and training requirements; ensure users meet required security investigation, clearance, authorization, mission requirement, and supervisory approval before granting access to the USU IS; ensure users receive initial and annual Cyber Security awareness training; ensure implementation of the Cyber Security Vulnerability Management Program, to include alert dissemination, component reporting, and compliance reporting; ensure that all ISs within their Area of Responsibility are certified, accredited and reaccredited; and to ensure log files and audits are maintained and reviewed for all systems.

2.3 Network Administrator/System Administrator (NA/SA)

A Network Administrator/System Administrator is appointed for each installation network or end-user system, and must meet the Information Technology (IT) designation, security clearance, and training requirements applicable to the assignment. A NA/SA's main function is to ensure that the USU IS infrastructure remains operational and secure. This person will conduct reviews of the network architecture for vulnerabilities, report security violations and incidents to the Cyber Security Manager, review and evaluate the effects on security of changes to the network, perform required monitoring of network resources, and analyze and maintain network audit data.

2.4 NOC Cyber Security Personnel

NOC Cyber Security Personnel, to include those specified above, have crucial responsibilities within NOC. Personnel with these responsibilities include all IT staff with responsibilities relating to the USU IS. They enforce the IS security guidance policies; oversee system access, operation, and maintenance; review user account accesses and logins and suspend suspect or inactive accounts; and ensure configuration management (CM) policies are followed, to include all pertinent patches and fixes, maintaining anti-virus, establishing audit trails, conducting reviews, and creating archives.

3. ACCESS CONTROLS

Access control is the process by which users are identified and the SAs either permit or deny the use of a particular USU IS resource. The SAs only provide access to personnel once a signed System Authorization Access Request (DD Form 2875), that verifies a user's security clearance level and need-to-know, Cyber Security Awareness and Training Certificate, and USU Computer User Agreement document is received. The USU IS requires each user to provide a unique user ID and password combination, Common Access Card (CAC) credential, or some other form of two-factor authentication, before accessing the system, either initially or after a screen has been locked.

When an employee departs the organization, they must be out-processed through the USU Service Center in order to delete their access credentials.

The basics of access control are to manage proper disclosure of information to USU personnel. USU follows the least privilege approach, which ensures that users log on with limited user accounts to perform day-to-day operations, and restricts administrative tasks to only those individuals who authenticate with administrative credentials.

3.1 Access Control List (ACL)

The NOC ACL is used to provide permissions or access rights to a particular computer resource, file, or directory for each user to the operating system through Active Directory.

3.2 Permissions

Permissions identify the type of access granted to a user. For example, the Security Engineer group can be granted Read and Write permissions for a file named (example) SecEngr.dat or other files pertaining to Security Engineering. Permissions are applied to any objects such as files, Active Directory (AD) objects, or registry objects. Permissions can be granted to any user, or computer. Common permissions are:

- Read permissions
- Modify permissions
- Change owner
- Delete

3.3 Monitoring

Consent to Monitor: All personnel using a Government computer must consent to monitoring. On some systems, a CAC may be used to log in, and if so, the user may be able to simply click "OK" or type in a Personal Identification Number (PIN) to establish a connection (some systems or web sites will perform this function automatically). A USU computer is provided to a user for authorized use only. USU computers are monitored to ensure that use is authorized and that users follow security procedures. Monitoring is also performed to ensure hackers have not gained access to computers. Privacy does not exist on USU computers and users should therefore not expect it.

3.4 User Account Management

Microsoft Active Directory is used to manage user accounts, computers and groups. AD has a wealth of information and facilitates tracking user activity such as logon/logoff, identifying inactive or disabled user accounts which can compromise the security of the network, and tracking user account status, such as when it is going to expire, when there should be a password change and what permissions users have. Being able to generate comprehensive reports by extracting the data from AD for all these aspects can give insights on the user life cycle in an organization. These reports will be useful to personnel auditing the system to verify if pre-defined organizational policies and regulatory compliance requirements are met or not.

3.5 Principle of Least Privilege (POLP)

NOC Cyber Security Personnel will limit access to IS resources only to those authorized users, programs, process, or other systems using the POLP via automated or manual means.

a. User account management includes maintaining complete user account forms, reviewing accounts periodically to determine whether access is still necessary, and reviewing user activity to ensure that only authorized users can gain access to workstations, applications, and networks. Access to all shared file systems is limited to the personnel identified as authorized by the organization and those that have a valid need-to-know.

b. Successive logon attempts are denied when access has been locked after three unsuccessful logon attempts; the number of access attempts in a given period is limited and an account disabling system is employed.

3.6 Privileged Users

Privileged user accounts enforce a restrictive access policy for their privileged technical users, provide a standardized containment for privileged users that satisfy access control requirements for compliance, and effectively track all privileged user activities and events with comprehensive and real-time reporting for accountability.

3.7 Role-Based Access Control (RBAC)

RBAC is an approach to restricting system access to authorized users. It is an alternative approach to MAC and DAC. RBAC is sometimes referred to as role-based security.
Staff and other system users are assigned particular roles which are created for various job functions. Permissions to perform certain operations are assigned to those specific roles. User's roles are determined by their responsibilities and qualifications and the users roles can be reassigned from one role to another. Roles can be granted new permissions as new applications and actions are incorporated, and permissions can be revoked from roles as needed.
RBAC is used to ensure users have discretionary access to only those enterprise objects that they have been granted access to. This type of permission simplifies authorization and provides flexibility in specifying specific protection policies.

3.8 Group Authenticators

The design of some systems necessitates more than one individual using the same identifier/authenticator combination for application or network access. Such situations are often

referred to as requiring the use of group authenticators. The use of group accounts must be approved by the Cyber Security Manager.

a. A form will be completed to collect a unique identifier for each person who will have access to the group authenticator, which will ensure positive identification of authorized users of the group authenticator. This form is then provided to the Cyber Security Manager.

b. General Guidelines for Group Authenticators:

1) Group authenticators must be approved by the Cyber Security Manager prior to implementation.

2) Group authenticators may not be shared with anyone outside of the group without the specific permission of the Cyber Security Manager.

3) When utilizing a logon ID as the identifier, passwords must follow the standards set in the Password Policy.

3.9 DoD Public Key Infrastructure Class 3 or 4 Certificate

Ensure that Identification and Authentication is accomplished using the DoD Public Key Infrastructure Class 3 or Class 4 certificate and hardware security token or NSA-certified product.

3.10 Database Transaction Recording

a. Ensure that access control mechanisms exist to ensure that data is accessed and changed only by authorized personnel.

b. When auditing, using the database transactions function, you are able to view historical information for a specific object (i.e., records, blocks, pages, segments, files, directories, directory trees, and programs, etc.) and compare the object's profile before and after a specific transaction occurred to determine what information was modified as a result of the transaction. You can access the transaction history for a profile or you can access transaction histories for one or more profiles.

3.11 Integrity of Hardware, Software and Firmware

a. The architecture depicts the security support structure as being isolated physically, using domains and partitions, and the security support products are configured securely to provide access controls and the integrity of the products.

b. The process of controlling modifications to a telecommunications or information systems hardware, firmware, software and documentation to ensure the system is protected against improper modifications prior to, during, and after system implementation.

4. AUDIT PROCESS

4.1 Audit Trail

An audit trail or audit log is a chronological sequence of audit records, each of which contains evidence directly pertaining to and resulting from the execution of a business process or system function. Audit trails preserve an activity record of the system to include changes to the system, operating system and application process events, and user activity on the system. SAs will configure the system to automatically log all access attempts. Several different types of tools are used to obtain these records and assist in detecting security violations, performance problems, and flaws in applications. SAs use the audit trails to ensure that the system or resources have not been harmed by hackers, insiders, or technical problems in support of USU IS operations.

4.2 Audit Permissions

4.2.1 Permissions for USU Personnel

To protect the audit logs from unauthorized access, modification or deletion, SA's set permissions on the system for privileged and general users.

a. The first permission set is for the privileged user; it gives the privileged user access to all the system controls, monitoring, or administrative functions, e.g., audit logs, application software, servers, and the server and workstation operating systems. Examples of privileged users are the Cyber Security Manager, SA or NA.

b. The second permission set is for the general user; it gives only limited access to the system, application software, software tools, and commercial office suite products, but cannot access or view any auditing functions. The general users may input information to or modify information on the system or can receive information from the system or from other systems. General users will not be given access to the system controls or administrative functions. Examples of general users are system operators or other system users that require limited access.

4.2.2 Permissions for Tenant Personnel

An outside organization with systems connected with the USU IS must enter into an agreement with USU for the purpose of performing an audit and will provide the NOC consent to access. The information below will be provided in either the Tenant Security Plan (TSP) or a Memorandum of Understanding/Memorandum of Agreement attached to the TSP.

The TENANT NAME provides its consent to allow the NOC to perform an INTERNAL or EXTERNAL audit and to access its networks and/or firewalls to the extent necessary to allow the NOC to perform the scans authorized in this agreement. TENANT NAME shall provide protocols, addressing information, and network connections sufficient for the NOC to utilize the software to perform network scanning. This access will include:

- User level and/or system level access to any computing or communications device.
- Access to information (electronic, hardcopy, etc.) that may be produced or stored on TENANT NAME equipment or premises.

- Access to work areas (labs, offices, cubicles, storage areas, etc.).
- Access to interactively monitor and log traffic on TENANT NAME networks.

By signing this agreement, all involved parties acknowledge that they authorize an INTERNAL or EXTERNAL audit to use their service networks as a gateway for the conduct of these tests during the dates and times specified.

4.3 Audit Record Content

The audit records include the following information:

- User ID.
- Successful and unsuccessful attempts to access security files (e.g. audit records, password files, access control files).
- Date and time of the event.
- Type of event.
- Success or failure of event.
- Successful and unsuccessful logons.
- Denial of access resulting from excessive number of logon attempts.
- Blocking or blacklisting a user ID, terminal, or access port and the reason for the action.
- Activities that might modify, bypass, or negate safeguards controlled by the system (SA logon, logging directly onto a router vs. using Terminal Access Controller Access Control System Plus (TACACS+), altering access control lists, or altering security files).
- Account creation or deletion.
- Identity of the IS Component where the event occurred.

4.4 Audit Trail Protection

DoD Instruction 8500.01, "Cyber Security Implementation," dated 06 February 2003, Cyber Security Control ECTP-1 requires that the contents of audit trails are protected against unauthorized access, modification, or deletion. The contents of audit log data can be protected in the following ways:

- Physical access to the device.
- Only the below classes of personnel are allowed access to audit logs. No other access is permitted:
  - SA Read access only.
  - Cyber Security Manager – authorized to delete the audit log after it is archived.
  - Include in the audit trail the identity of each entity accessing the system; time and date of the access; time and date the entity terminated access; activities performed using an administrator's identification; and activities that could modify, bypass, or negate the system's security safeguards.
  - Database auditing involves observing a database so as to be aware of the actions of database users. Implement access and auditing controls to protect database management systems from unauthorized accesses and activity.

4.5 Audit Trail Review

The following types of Audit Trail reviews are implemented:

- Audit Trail Review After an Event. Following a known problem, a known violation of existing requirements by a user, or some unexplained system or user problem, the SA will review the audit trails. Review by the application/data owner would normally involve a separate report, based upon audit trail data, to determine if their resources are being misused.
- Periodic Review of Audit Trail Data. The SAs will review audit logs and audit trails weekly; more frequently if required.
- Real-Time Audit Analysis. Traditionally, audit trails are analyzed in a batch mode at regular intervals (e.g., daily). Audit records are archived during that interval for later analysis. Event Log Analyzer will be used in a real-time for audit review.

4.6 Audit Reduction and Report Generation

a. Tools are available for the review of audit records and for report generation from audit records. The tools should allow customization of the set of reports for the existing compliance report and ensures that you submit only required reports you are able to:

- Add new reports
- Remove reports
- Customize reports
- Schedule a compliance report generation automatically

b. The tools will include alerts on event logs which notify administrators when an event matching specific criteria is generated. Alerting helps administrators monitor critical servers and processes on the network.

c. An automated, continuous on-line monitoring and audit trail creation capability with the capability to immediately alert personnel of unusual or inappropriate activity with potential Cyber Security implications, and with a user configurable capability to automatically disable the system if serious Cyber Security violations are detected is deployed.

4.7 Using Analyzer Tools

An analyzer tool or manual operation will be used for centralized audit collection for web- based, real-time, event monitoring, and management solutions that improve security and reduces down time of distributed servers and workstations on the enterprise network. Once an enterprise solution tool is chosen, it must be determined that the tool is on the approved products list before purchase.

4.7.1 Review of Audit Records and Report Generation

a. To collect, analyze, report, and archive, Event Logs from Windows hosts, SysLogs from Unix hosts, routers, switches, and other SysLog devices, application logs from web servers and Microsoft Structured Query Language (SQL) servers, perform these functions:

NOTE: The Splunk Audit Tool will automatically collect all audit data on the servers and devices.

- Consider all requirements to reduce system downtime and increase network performance in the enterprise by assisting SAs to troubleshoot performance problems on hosts, select applications, and the network.
- Find the applications causing performance and security problems.
- Determine any unauthorized access attempts and other policy violations.
- Identify trends in user activity, server activity, peak usage times, etc.
- Obtain useful event, trend, compliance and user activity reports.
- Understand security risks in your network.
- Monitor critical servers exclusively and set alerts.
- Understand server and network activity in real-time.
- Alert on hosts generating large amounts of log events indicating potential virus activity.
- Schedule custom reports to be generated and delivered to your inbox.
- Generate reports for regulatory compliance audits.
- Identify applications and system hardware that may not be functioning optimally.

4.7.2 Report Types

The types of reports that will need to be prepared and reviewed:

- User Logon Report: User access to a system is recorded and monitored for possible abuse with log-in monitoring. While the intent is to catch hackers, this report documents access by legitimate users as well.
- User Logoff Report: User access to a system is recorded and monitored for possible abuse with log-out monitoring. Recording/documenting access provides a possible deterrent of abuse since the user knows there is proof of his or her activity.
- Logon Failure Report: The security logon feature will include logging all unsuccessful login attempts. The user name, date, and time will be included in this report.
- Audit Logs Access Report: Regularly review records of information system activity such as audit logs.
- Object Access Report: Identify when a given object (File, Directory, etc.) is accessed, the type of access (e.g. read, write, delete), whether or not access was successful/failed, and who performed the action.
- System Events Report: Identifies local system processes such as system startup and shutdown and changes to the system time or audit log.
- Successful User Account Validation Report: Identifies successful user account logon events, which are generated when a domain user account is authenticated on a domain controller

- Unsuccessful User Account Validation Report: Identifies unsuccessful user account logon events, which are generated when a domain user account is authenticated on a domain controller.

4.7.3 Audit Record Retention

NOC Cyber Security Personnel collect and retain audit data for at least one year. The records must be retained in sufficient detail to reconstruct events in determining the causes of compromise and magnitude of damage should a malfunction or a security violation occur. Audit records are available and stored off-line. These records are used to provide this data to appropriate law enforcement or other investigating agencies, support technical analysis relating to misuse, penetration reconstruction, or other investigations, and archive all event logs and syslogs collected from Windows hosts, routers and switches, and other syslog devices. Archive requirements include creating an archive file every 24 hours, loading archived event logs into a database, if possible, and generating reports from the event data archived. The policy of the USU is to ensure that operating systems are configured not to overwrite (or otherwise lose) audit trails when the log lengths reach specified maximums.

4.8 Audit Logs

Audit logs are composed of log entries; each entry contains information related to a specific event that has occurred within a system or network. Audit logs are consolidated using audit servers to manage, monitor and report on audit data for a complete view of enterprise data access. IT security and audit personnel must have the ability to analyze audit data in a timely fashion across different systems.

4.9 Audit Trail Backup

USU has integrated the data into the daily and weekly backup plan. All data is backed up, and is available for restoration.

4.10 Auditing Remote Access (RAS)

RAS for privileged functions is controlled and allowed only for compelling operational needs that are clearly documented and defined. These privileged remote users will be connecting to a DoD core network to perform any SA duties, to include troubleshooting, performing configuration changes, and reviewing any system or configuration data, regardless of system type. Determine which computers offer remote access services, then ensure that remote RAS auditing is possible and manually perform this check.

5. CYBER SECURITY VULNERABLE MANAGEMENT

The Cyber Security Branch must ensure that a Cyber Security Vulnerable Management Plan has been created, updated, and is strictly adhered to by NOC Cyber Security personnel. This plan describes to the Government and contractor users how security updates, patches, and policies should be updated throughout the life cycle management of the system. All members of NOC Cyber Security are responsible to know there is a plan, have a documented copy, and be able to perform the functions required by the plan. The goal of the Cyber Security Vulnerable Management Plan is to play a part in attaining and sustaining operational resiliency in the overall NOC Cyber Security program.

a. Cyber Security Vulnerability Alerts are issued through USCYBERCOM. Technical Cyber Security Alerts provide timely information concerning current security issues, vulnerabilities, and exploits. Cyber Security Vulnerability Alerts are computer application software or operating system vulnerability security bulletins, determined by DoD-CERT, considered to be mandatory for the baseline operation of all DoD computer systems. A subscription to these alerts can be found on the CERT web page http://www.us-cert.gov/cas/alldocs.html.

b. The Cyber Security Vulnerability Plan explains how personnel will test and implement issued Cyber Security Vulnerability Alerts.

NOTE: See USU Instruction 7900, Addendum L, CSVM Program policy for additional information on the CSVM program.

5.1 Scans

Scans test the integrity of equipment attached to the network and reduce the threat to the USU IS by identifying vulnerabilities.

- CSVM Compliance scanning and reporting definition: According to BBP 04-EC-O-0004 Network Assessment Scanning, "CSVM compliance is the absolute minimum standard for all ISs, not the preferred end-state. The end-state is a proactive methodology of maintaining, patching, or updating systems to prevent exploitation in advance of published CSVM messages and verification of policy requirements. CSVM does not always address IS vulnerabilities or services that pose a significant risk to the IS or network."

5.1.1 Types of Scans

a. Port Scanning: A port scan is conducted when an auditing program attempts to make connections to ports on a scanned system for the purpose of identifying which ports are active on the system. The scan will send packets, analyze replies, and will retrieve device information concerning the inventory of assets. The scan may also collect information showing the device IP address, the operating system, service pack level, build level, and machine name of the device found. Depending on the type of scan run, the program will present several types of reports that NOC Cyber Security personnel may use to analyze system problems or tighten system security. Port scanning is an information gathering process, and when performed by unknown individuals it is considered a prelude to attack.

b. Vulnerability Scanning: Vulnerability scanning is the process of identifying known vulnerabilities of computing systems on the network. Vulnerability scanning can be used to help secure the network or can be used by intruders to identify weaknesses in the system. The vulnerability scan can identify devices on the network that are open to known vulnerabilities. NOC Cyber Security personnel may run scans to identify and fix these weaknesses before an intruder finds the weakness and can mount an attack. See BBP 04-EC-O-0004 Network Assessment Scanning for rules on running these scans since there may be a possibility of causing a system crash.

5.2 Compliance Testing

Compliance testing is performed to test all patches, upgrades, and new IS applications prior to deployment. A comprehensive set of procedures are in place in the CM Plan to describe the required compliance testing.

5.3 Purpose

The purpose of performing periodic network scans is to test the integrity of the USU IS. The goal of the scans is to reduce the vulnerability of USU IS network equipment and computers to hacking, denial of service, infection, and other security risks from both inside and outside USU. The following are applicable scanning tools:

a. For Windows systems, staff implementing Cyber Security Controls should know about the following:

- Security Technical Implementation Guide (STIG) – STIGs are used to provide the technical security policies, requirements, and implementation details for applying security concepts to commercial off-the-shelf applications. It should be noted that some security controls may break some critical functions; therefore, testing before applying to the live system is mandatory. If implementation of a STIG negatively impacts system functionality, an application for risk awareness and acceptance must be submitted to the DAA, and the resulting decision must be followed and a record obtained for future reference.
- Security Configuration Guide (SCG) – Cyber Security Control ECSC-1, Security Configuration Compliance, directs the use of security guides and STIGS. The Defense Information Systems Agency (DISA) and the National Security Agency (NSA) have security guides for Windows and accompanying applications. Implementation of these guides will also satisfy many of the other Cyber Security Controls besides ECSC-1. Check this web site for the security guides and other information: http://iase.disa.mil/stigs/index.html.
- Gold Disk - Scans for CAT I, II and III vulnerabilities according the applicable Mission Assurance Category (MAC) level. With the Gold Disk, you need to check for false positives. Also, some Category Is and IIs may not be fixable.

b. For UNIX/Linux Systems: There is no standard configuration for any UNIX environment. The UNIX Security Readiness Review (SRR) Scripts are supported on the following platforms and versions: Solaris 2.5.1 through Solaris 10; HP-UX 11.0, HP-UX 11.11; Red Hat Enterprise Linux 3 and 4; and AIX 4.3:

- STIG – See above
- Security Configuration Guides – See above
- SRR - UNIX has an automated script called the SRR. Running the script requires skills in the command line. SRR scripts pick up false positives so the technician/engineer running the script needs to know what is running on the system and what does not need to be running. UNIX knowledge is a must to use the SRR effectively.

5.4 Service Degradation and/or Interruption Notifications

a. Normal Operations: Planned scans, system updates, and maintenance will be announced five days in advance via email from Cyber Security staff. Operational and support statistics will be reported monthly.

b. Unexpected Interruptions: In the event of unexpected service interruption, NOC Cyber Security personnel will send notification via the service desk, of service interruption within 15 minutes of the identification of loss of service. Status updates will be provided on an hourly basis on the system status page to subscribed individuals. Service interruption information will be released after the resolution of the interruption.

6. ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action, up to, and including termination of employment. Systems that are not compliant with this policy, risk disconnection until compliance is met.

WIRELESS LOCAL AREA NETWORKS (WLANs)

1. Purpose.

The purpose of this policy is to:

a. Support references *(a)* through *(m)* concerning wireless transmission of all USU data over a wireless 802.11X LAN. The protection of all wirelessly transmitted data and packet information, to include source and destination Internet Protocol (IP) addresses, mitigates the risk of compromising Sensitive Information (SI), Personal Identifiable Information (PII) or Protected Health Information (PHI) over a wireless network connection.

b. Assign responsibilities to ensure that sufficient defense-in-depth security safeguards are implemented to prevent the compromise of one system's security assurance by vulnerabilities of interconnected systems introduced via wireless communications.

c. Promote interoperability using open standards for commercial wireless implementations throughout USU.

d. Promote the use of a Knowledge Management (KM) process for the sharing of wireless technology capabilities, vulnerabilities, and vulnerability mitigation strategies throughout USU.

2. Scope.

This policy applies to all USU employees to include faculty, staff, students, and contractors that utilize and/or manage USU IS. In addition, this policy applies to all temporaries and guests who are authorized to temporarily utilize USU IS.

This policy incorporates existing Defense Information Systems Agency (DISA), Health Insurance Portability and Accountability Act (HIPAA) Security Rule, and Service policy and guidance with USU-specific guidance to provide a foundation for a comprehensive risk mitigation strategy that ensures sensitive data, including PHI/PII, transmitted via wireless technology is protected from unauthorized disclosure and that the introduction of Wireless Local Area Networks (WLANs) into the DoD environment protects DoD networks from unauthorized access and other malicious attacks.

a. This policy applies to all USU data transmitted via a wireless connection except as noted below.

1) Examples of USU data include, but are not limited to the following: official email transmissions; SI/PHI/PII data covered under the Privacy Act; data designated as "Unclassified/For Official Use Only;" and procurement of SI. This includes data transmitted wirelessly to and from medical devices (e.g., handheld order-entry devices, medical monitoring devices, Portable Electronic Devices (PEDs), Personal Digital Assistants (PDAs)).

2) Wireless connections typically include, but are not limited to, the 802.11 Institute of Electrical and Electronics Engineers Standard for WLA.

3) Bluetooth devices shall not be used to store, process, or transmit DoD information unless Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements for Cryptographic Modules," dated December 3, 2002 compliant cryptographic modules are used to encrypt the data during transmission.

4) The USU Wireless Policy does not apply to wireless transmissions to or from receive-only pagers, Global Positioning System (GPS) receivers, hearing aids, pacemakers, other implanted medical devices, or personal life support systems. The detection segment of a PED (e.g., the laser beam between a laser disk and its reader head; between a barcode and a scanner head; or radio frequency (RF) energy between wireless identification tags, both active and passive, and the reader/interrogator) does not require encryption.

b. This document should be used in conjunction with policy, directives, and Cyber Security measures for wireless implementations from DoD, DISA, National Security Agency (NSA), the Services, and USU to protect data on Wireless Local Area Networks (WLANs) and portable devices.

3. Policy.

It is USU Policy that:

a. Acquisitions for new and/or upgraded equipment used for the transmission of USU data utilizing 802.11 wireless technology using Defense Health Program (DHP) or research grant funds must meet the minimum requirements outlined in this document.

b. Additional publications are listed in Appendix A of the DISA Security Technical Implementation Guide (STIG) regarding wireless policies, guidance, standards and vulnerabilities, and Wired Equivalency Privacy (WEP) vulnerabilities.

1) References *(a)*, *(b)*, and *(c)* identify the minimal implementation requirements of wireless technologies for the transmission of information on DoD networks. These references provide guidance for two categories of wireless device usage. The WLAN Technology section discusses wireless networking technologies and associated security policies. The Remote Wireless Networking Technologies section discusses remote access devices, such as mobile telephones and personal data devices, two-way pagers, and e-mail devices.

2) Wireless devices and systems that do not meet the security requirements of references *(d)* and *(e)* should not be used to store, process, access, or transmit DoD information unless approved by the Designated Approving Authority (DAA) as necessary to meet specific mission requirements.

3) The Site DAA shall ensure that DoD, USU, and Service-specific guidance regarding implementation of wireless infrastructure, transport, and storage of PII/PHI data are followed. The site DAA shall ensure procedures are developed and followed for safe implementation, intrusion detection, and monitoring of wireless technologies. See reference *(f)* for additional recommendations and industry best practices for the mitigation of wireless risks

c. Data Encryption. Encryption of data for transmission to and from wireless devices is required. Exceptions may be granted on a case-by-case basis as determined by the DAA. At a minimum, data encryption must be implemented end-to-end over an assured channel and shall be validated under the Cryptographic Module Validation Program as meeting requirements for FIPS Pub 140-2 Overall Level 1 or 2.

d. Wireless transmission of classified information is prohibited.

e. Lost or Stolen Devices with Wireless Capability. The loss or theft of any device with wireless capability should be immediately reported to the Cyber Security Officer or designated individual. Remote network access by the device should be immediately deactivated upon notification of the device reported as lost or stolen.

f. Disruption and Interference. All newly deployed wireless technologies must satisfy all existing standards as required by DoD, Federal, and local Service policy, with particular attention for medical, safety, and emergency devices.

g. User Training Program

1) Ensure that users on the network are fully trained in computer security awareness, HIPAA privacy and security, and the risks associated with wireless technology.

2) Ensure that visitors to the site are made aware of wireless device usage and wireless transmission of data.

h. Intrusion Detection. Implementation of a fully automated wireless rogue detection system is strongly recommended.

i. Wireless technology implementation integrated or connected to USU networks are considered part of those networks, and must comply with DoD Directive 8500.1 and be certified and accredited in accordance with DoD Instruction (DoDI) 5200.40, "DoDI 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)."

j. Wireless technologies for transmitting information shall not be operated in areas where classified information is electronically stored, processed, or transmitted unless approved by the DAA, in consultation with a Certified TEMPEST Technical Authority (CTTA). The responsible CTTA shall evaluate the equipment using risk management principles and determine the appropriate minimum separation distances and countermeasures.

k. Introduction of wireless communications for the transmission of USU data can have a significant adverse effect on the security posture of the information system (IS). A security review and documentation should be conducted in accordance with DoDI 5200.40 and the HIPAA Security Rule.

l. Transfer of data via infrared ports should be avoided where possible to minimize inappropriate access to USU data. Protected methods of data transfer should be utilized when feasible. If transfer of USU data via infrared is required, the infrared ports should be adjacent to each other for the duration of the transmission.

m. Preventive measures shall be taken to mitigate denial of service attacks. These measures shall address not only threats from the outside, but potential interference from friendly sources, such as microwave ovens.

n. Active screening for wireless devices shall be conducted to detect/prevent unauthorized access of USU Component information.

4. Procedures.

Wireless network devices extend network accessibility by reducing the requirements of the physical infrastructure needed in the traditional wired network. Vulnerabilities of wired networks apply to wireless ones as well. However, the unique properties of the wireless network introduce several vulnerabilities that warrant additional security analysis. Removing the traditional physical constraints of wired networks makes intrusion detection more difficult, and makes eavesdropping and denial of service attacks potentially easier.

Since wireless signals are radio transmissions, they can be intercepted by radio receiving devices, even devices outside of the intended service area. If data transmissions are not adequately protected, the intercepted data can be read and understood in a matter of seconds.

Wireless transmissions circumvent traditional perimeter firewalls. Technological advances in wireless signaling may increase transmission distances, further increasing the problem of unauthorized reception. Improper implementation of a wireless network may allow an unauthorized user access to wired networks and the data and assets residing on it. Without appropriate Cyber Security measures, DoD networks are faced with the potential of growing numbers of unauthorized users looking for rogue access points.

Differences between protocols in the 802.11 family are not significant with respect to security. The 802.11 WLANs all use the same layer 2 packets; the difference is in the physical layer. Attacks on WLANs have become more prevalent and easier with the wide array of publicly available tools. This situation emphasizes the need for secure implementation of wireless technologies and constant vigilance against intrusion related activities from unauthorized sources.

a. Protection and mitigation strategies for USU data during transmission via wireless 802.11x LAN technologies, regardless of transmission method, should include:

1) Data in transit via traditional wired Wide Area Networks/Metropolitan Area Networks/Local Area Networks (WAN/MAN/LAN).

2) Data at rest.

a) Stored on portable devices (e.g., laptops, Blackberry devices).

b) Stored on workstations.

c) Stored on application storage devices.

3) Authentication and access control procedures for networks, applications and portable devices.

a) Password and encryption protection mechanisms.

b) Logon passwords.

c) Timed log-out features.

4) HIPAA-related concerns.

a) Audit requirements.

b) HIPAA security awareness training.

c) The Cyber Security Manager roles and responsibilities.

5) Disposal of data storage and portable devices.

a) The primary areas of concern for mitigation of security risks when incorporating a wireless solution into a wired network include, but are not limited to:

(1). Internal Threats

(a). Unauthorized undetected access.

(b). Accidental association to neighboring networks.

(c). Insecure configurations.

(1) Default passwords.

(2) Weak encryption.

(3) Weak authentication.

(4) Broadcasting of Service Set Identifier (SSID).

(5) Lost or stolen devices.

(6) Media Access Control (MAC) spoofing.

(2). External Threats.

(a). Scanning, snooping, and probing.

(b). WEP and Extensible Authentication Protocol (EAP) attacks.

(c). MAC spoofing.

(d). AP association attacks.

(e). Redirection attacks.

(f). Denial of Service (DoS) attacks.

(g). Springboard attacks.

5. Responsibilities.

a. USU Chief Information Officer (CIO) shall:

1) Provide oversight guidance for wireless transmissions of USU data.

2) Provide analytical and standards support to the USU Components concerning proper employment of wireless technologies.

b. DAAs or the designated representatives shall:

1) Ensure that all new commercial wireless procurements comply immediately with the provisions of this guide.

2) Implement accountability, access control, and audit trail methods to track and actively monitor wireless transmissions of USU data. The type of transmission authorized and associated network utilized for all USU Component communications must be identified and documented.

3) In accordance with the DoD Cyber Security Certification & Accreditation Process (DIACAP):

a) Control wireless transmissions of USU IS data under their cognizance to ensure the wireless solutions (including external interfaces to commercial wireless services) do not introduce vulnerabilities undermining the assurance of the other interconnected systems.

b) Ensure wireless interfaces are consistent with Federal, DoD, and local Service policies.

4) Ensure wireless Personal Area Networks (PANs) (e.g., Bluetooth) capabilities are removed or physically disabled from a device unless FIPS Pub 140-2 validated cryptographic modules are implemented.

5) Promote the use of wireless KM processes when evaluating potential wireless solutions.

6) Develop a local Wireless Device Usage Statement specific to their activity for End-users. *(See Attachment 1 for a sample statement.)*

7) Provide initial and ongoing security training specifying precautions for use of wireless communications.

c. Users shall:

1) Adhere to USU and local Service policy for wireless devices.

2) Immediately report to Cyber Security any suspected compromise of USU data transmissions.

3) Sign a Wireless Device Usage Statement specific to the local activity signifying an understanding of the procedures and policies for wireless devices. *(See Attachment 2 for a sample statement.)*

6. References.

a. DoDD 8100.2, "Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)," April 14, 2004

b. Defense Information Systems Agency (DISA) Wireless Security Technical Implementation Guide (STIG), Version 2, Release 1, July 10, 2003

c. Defense Information Systems Agency (DISA) "Wireless Security Checklist," Version 2, Release 1.1, July 30, 2003

d. DoDI 8500.01, "Cyber Security," March 14, 2014

e. National Institute of Standards and Technology (NIST) Special Publication 800-48, "Wireless Network Security: 802.11, Bluetooth and Handheld Devices," November 2002

f. DoDD 8100.1, "Global Information Grid Overarching Policy," September 19, 2002

g. DoDI 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014

h. FIPS Publication 140-2, "Security Requirements for Cryptographic Modules," December 3, 2002

i. Public Law 104-191, "Health Insurance Portability and Accountability Act of 1996," August 21, 1996.

j. Privacy Act of 1974 (5 US Code Sec. 552a

k. DoD 6025.18-R, "DoD Health Information Privacy Regulation," January 2003

Attachments:
1. Wireless Device Usage Statement
2. Wireless Devise Use Agreement

WIRELESS DEVICE USAGE STATEMENT

Wireless Device Information

1. Manufacturer: _____ Model: _____ Serial Number: _____

2. Software Installed on Wireless Device: _____

3. Department where Wireless Device will be located/used: _____

4. Local Area Network System to be connected to: _____

5. Property Account Number of CPU or designated server on which wireless device software will be installed:

_____

Wireless Device Usage

a. Wireless Devices:

1) Shall be secured when not in use.

2) Shall only be connected to the identified Local Area Network listed above.

3) Shall conform to DoD policies of operation for information systems.

4) May be used to take notes, save information, or write e-mails while away from wireless device user's desk.

5) May be used to synchronize information with the wireless device user's desktop workstation using direct connect cables.

b. Wireless devices shall NOT be:

1) Used to process or store classified information.

2) Connected to any classified information system or network.

3) Used with modems to exchange information with wireless device user's desktop or other systems on the network.

4) Used to synchronize any equipment features or devices across any network.

5) Used to download and install freeware or shareware software enhancements to wireless devices. Such software is from untrusted sources and may contain malicious code.

6) Used for storing, processing or transmitting SI or PHI without explicit written approval of the DAA.

7) Left unattended while attached to a government information system.

c. Please contact your Cyber Security Officer if you have any questions or require additional information.

Wireless Device Use Agreement

1. I have read and understand the security guidelines for wireless device usage.

2. I understand the necessity for safeguarding my wireless device and recognize the requirement for maintaining confidentiality of all data stored in it.

3. I agree to abide by all of the Wireless Device Usage statements above and understand that failure to comply shall result in the loss of my wireless device use privilege.

4. I agree to abide by the Privacy Act of 1974 (5 U.S.C. 552a) that requires Federal agencies to safeguard personal data processed by and stored on wireless devices or technologies.

5. I agree to abide by the Health Insurance and Portability Accountability Act of 1996 (PL 104-191) and the DoDD 6025.18-R Health Information Privacy Regulation.

6. I shall immediately contact my Cyber Security Manager if I suspect a compromise of the device, the data it contains, or the transmission of data to or from the device.

User Information

Name:

Title:

Date:

Signature:

DATA INTEGRITY

1. Purpose.

This policy outlines safeguards for detecting and minimizing inadvertent modification or destruction of data. Data integrity is a security principle that ensures the continuous accuracy of data and information stored within networked systems. Data integrity is defined as the condition that exists when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed. Continuity of data integrity is paramount in the USU IS environment and is a key concept of the Defense-in-Depth strategy. System integrity is defined as the attribute of an IS when performing its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

Data must be kept from unauthorized modification, forgery, or any other form of corruption, such as from malicious threats or corruption that is accidental in nature.

Upon receiving and processing Sensitive Information in a USU IS, integrity must be verified to ensure that the information has not been altered, modified, or added to, or subtracted from, in transit by unauthorized users. Integrity has two main objectives:

a. Ensure that the data has not been altered in an unauthorized manner while in transit, during storage, or while being processed.

b. Ensure that a system, while performing its intended processes and applications, provides support to authorized users free from unauthorized manipulation. Exploitation of vulnerabilities associated with data or system integrity may result in a disruption or denial of service, and/or unauthorized modification of user or network information and network services. Data and system integrity requires implementing protection mechanisms as a means of preventing unauthorized modification or destruction of information. It is the responsibility of the USU Cyber Security Program Office to ensure protective measures are in place, coupled with industry best practices, to maintain the appropriate level of data and system integrity.

2. Scope.

This policy applies to all USU employees to include faculty, staff, students, and contractors that utilize and/or manage USU IS. In addition, this policy applies to all temporaries and guest who are authorized to temporarily utilize USU IS.

3. Policy.

USU requires implementing data and system integrity measures to protect DoD data from unauthorized manipulation, intentional or unintentional alteration, or destruction. Instituting access control mechanisms, utilizing virus protection programs, and establishing an information security monitoring capability are required measures, in accordance with Defense-in-Depth, to help protect the integrity of DoD data and systems.

It is USU Policy that:

a. The Cyber Security Officer shall ensure that access to all DoD and USU information is determined by its classification, sensitivity, and need-to-know. Need-to-know is established by the information owner and is enforced by discretionary or role-based access controls.

b. The Cyber Security Officer shall ensure policies and procedures are implemented for ISs that handle DoD data to allow access only to those persons or software programs that have been granted access rights.

c. The Cyber Security Officer shall establish and enforce access controls for all shared or networked file systems and internal web sites, whether classified, sensitive, or unclassified.

d. All internal classified, sensitive, and unclassified web sites shall be organized to provide at least three distinct levels of access:

1) Open Access – General information made available to all DoD and USU Component authorized users with network access. This access does not require an audit transaction.

2) Controlled Access – Information made available to all DoD and USU Component authorized users upon the presentation of an individual authenticator. This access shall be recorded in an audit transaction.

3) Restricted Access – Need-to-know information made available only to an authorized community of interest. Authorized users must present an individual authenticator and have a demonstrated or validated need-to-know. All access to need-to-know information and all access attempts shall be recorded in audit transactions.

e. The Cyber Security Officer shall establish appropriate control mechanisms to ensure that data at rest or in transit is properly disposed of by authorized personnel only.

f. The Cyber Security Officer shall establish and enforce procedures to verify the identity of a person or entity seeking access to data.

g. The Cyber Security Officer shall maintain and enforce procedures to establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

h. The Cyber Security Officer shall ensure that a controlled interface is implemented for interconnections among DoD ISs operating at different classifications levels or between DoD and non-DoD systems or networks.

i. The Cyber Security Officer shall determine the need for and the strength of the mechanism for automatic logoff based on DoD direction and the organization's risk assessment, and shall document policies and procedures for terminating an electronic session after a predetermined time of inactivity.

j. The Cyber Security Officer shall determine the appropriate mechanism for encrypting and decrypting sensitive electronic data and protected health information at rest and in transit in accordance with Federal Information Processing Standards (FIPS) 140-2, "Security Requirements for Cryptographic Models," dated December 3, 2002 and DoDI 8500.01.

k. The Cyber Security Officer shall implement system resource control and object access to ensure that all authorizations to the information contained within an object are revoked prior to initial assignment, allocation, or reallocation to a subject from the system's pool of unused objects. No information, including encrypted representations of information, produced by a prior subject's actions is available to any subject that obtains access to an object released back to the system. There must be no residual data from the former object.

l. The Cyber Security Officer shall implement electronic mechanisms to confirm that data has not been altered or destroyed in an unauthorized manner.

m. Virus protection shall be installed, enabled, maintained, and have the ability to be automatically updated on all USU ISs.

n. USU Components shall review system records on a weekly basis, or more frequently if deemed necessary.

o. USU Components shall implement and maintain an information security monitoring capability to ensure that all systems they operate and/or control are regularly monitored and protected by intrusion detection systems.

p. Successive logon attempts shall be controlled using one or more of the following:

1) Access is denied after three unsuccessful logon attempts in accordance with Chairman, Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-In-Depth: Cyber Security and Computer Network Defense (CND)," dated March 25, 2003.

2) The number of access attempts in a given period is limited.

3) A time-delay control system is employed.

4) The system provides a capability to control the number of logon sessions if the system allows for multiple-logon sessions for each User Identification (User ID).

4. Procedures.

a. The Cyber Security Officer shall manage authorized user accounts for USU systems, including configuring access controls to enable access to authorized information and removing authorization when access is no longer needed. The responsibility may be delegated to the System Administrator.

b. Limit users to three attempts when logging onto a USU IS. After the maximum number of incorrect attempts, the system shall lock out the user until an administrator unlocks the account.

Action from the Cyber Security Officer shall be required to reactivate the account. This action prevents outsiders from accessing the IS by using a known User ID and trying to guess the password.

c. Enable screen-lock functionality on all USU workstations and any workstation that accesses DoD information. When activated, the screen-lock function places an unclassified pattern onto the entire screen of the workstation, hiding what was previously visible. Such a capability is enabled by either explicit user action or a specified period of workstation inactivity (e.g., fifteen minutes). Once the workstation screen-lock software is activated, access to the workstation requires knowledge of a unique authenticator. Special accommodations (i.e. longer 30 minute time-outs) for workstations in teaching space such as lecture halls can be made when approved by the DAA and reviewed annually.

d. The screen lock function shall not be considered a substitute for logging out (unless a mechanism actually logs out the user when the user idle time is exceeded).

e. In addition to DoD 5500.7-R, "Joint Ethics Regulation (JER)," requirements, the Health Insurance Portability and Accountability Act Security Rule provides specific security standards for the protection of workstations that process protected health information. These include:

1) Locking the workstation before leaving the workstation unattended.

2) Position workstation to obstruct unauthorized viewing and access.

f. The Cyber Security Officer shall establish web site administration policy and procedures consistent with the "DoD Web Site Administration Policies and Procedures," (SOP) November 25, 1998, as amended on January 11, 2002.

g. The Cyber Security Officer shall establish system Access Control Lists to restrict traffic to only that which is required to pass through the web site.

h. All USU IS users shall take precautions to prevent viruses from infecting USU ISs. The Cyber Security Officer shall ensure all developers are protecting source or executable code by utilizing 'checksum' or another safeguard to ascertain that approved code is not altered.

i. The Cyber Security Officer shall ensure all software loaded on a system is first scanned for viruses.

j. All USU IS users are to report suspected virus activity to the local supervisor or Cyber Security Officer.

Suspicious activity includes, but is not limited to:

1) Suspected misuse or unauthorized use of government resources.

2) Use of an IS account and password by another party.

3) Illegal copying of software.

4) Abnormal activity on an IS, which may indicate the presence of a computer virus or malicious code.

k. Only approved, virus scanned software shall be installed on workstations.

l. No software that changes the security posture shall be installed on USU ISs without approval from the Designated Approving Authority.

m. The Cyber Security Officer shall ensure that backup copies of protected system files, critical data files, and applications (backup copies of applications for archival purposes generally do not represent a copyright violation) are created and stored on electronic storage media in a secure location and are not collocated with the originals. A network/system administrator should have a backup copy of every software program each time it is modified in accordance with established software development procedures and controls. This provides some assurance that a clean backup exists in the event a virus or malicious code is detected. The system administrators should also periodically scan the servers for viruses or malicious code.

n. The Cyber Security Officer shall ensure encryption and decryption standards are in compliance with the FIPS Pub 140-2 and DoDI 8500.01. The Cyber Security Officer shall require and ensure encryption policies and procedures are documented.

o. Users shall not use electronic storage media from home systems or other external sources that have not been approved and scanned for viruses. Users shall not duplicate copyrighted software or share software with other employees.

p. In case of an incident or catastrophic failure, routine data backup and detailed disaster recovery plans shall be available to retrieve exact copies of lost data and ensure data integrity.

q. Users shall be trained annually, at the minimum, on appropriate security practices for operating a USU workstation and IS. Security practices include guarding against, detecting, and reporting malicious software, as well as monitoring and reporting unauthorized logon attempts.

5. References.

a. CNSSI No. 4009, "National Cyber Security Glossary," May 2003

b. CJCSM 6510.01, "Defense-In-Depth: Cyber Security and Computer Network Defense (CND)," March 25, 2003

c. DoDI 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014

d. DoD 5500.7-R, "Joint Ethics Regulation (JER)," August 1993 (Changes 1-4)

e. DoDI 8500.1, "Cyber Security," March 14, 2014.

f. Federal Information Security Management Act of 2002.

g. FIPS Publication 140-2, "Security Requirements for Cryptographic Models," December 3, 2002.

h. NIST SP 500-170, "Management Guide to the Protection of Information Resources," October 1989.

i. NIST SP 800-27, "Engineering Principles for Information Technology Security (A Baseline for Achieving Security)," Revision A, June 2004.

j. NIST SP 800-47, "Security Guide for Interconnecting Information Technology Systems," September 2002.

k. Public Law 104-191, "Health Insurance Portability and Accountability Act of 1996," August 21, 1996.

l. "DoDI 8550.01,"DoD Internet Services and Internet-Based Capabilities," September 2012.

6. Revision History.

CHANGE / REVISION RECORD			
Date	**Page/Paragraph**	**Description of Change**	**Made By:**
May 2014		Annual Review	jrobertson

CERTIFICATION AND ACCREDITATION (C&A)

1. Purpose.

USU Certification and Accreditation (C&A) is a four-phase process consisting of definition, verification, validation, and post accreditation that applies to all the USU Component and contractor ISs, including networks. The USU C&A process is conducted in accordance with current DoD C&A guidance. The primary purpose of the USU C&A process is to protect and secure the elements that make up the USU information infrastructure, regardless of where the IS is located. The USU C&A procedures shall be utilized in conjunction with current DoD C&A guidance and DoDI 8500.01, "Cyber Security," dated March 14, 2014.

All DoD ISs shall be reaccredited within three years of the effective date of the system's Approval to Operate (ATO) or when significant changes occur to impact the security posture of the systems. The USU C&A process must be monitored and maintained throughout the system's development life cycle. Key information technology (IT) personnel shall adhere to the USU C&A process for any government-owned or contractor-owned IS that transmits, processes, stores, or accesses DoD unclassified information, DoD sensitive information, and/or connects to any DoD system or network during acquisition, operation, and throughout the system life cycle.

2. Scope.

This policy applies to all USU users to include faculty, staff, students, guests, contractors and volunteers that utilize USU IS resources.

3. Policy.

a. The USU shall conduct C&A for all USU ISs (government-owned or contractor-owned) that transmit, process, store, or access DoD sensitive information and/or connect to any DoD system or network. The USU Cyber Security Program also requires USU contractors to comply with C&A requirements. The USU shall utilize current DoD C&A guidance as its baseline to maintain a sound Cyber Security posture throughout the USU IS infrastructure. Throughout all the phases of USU ISs development, information owners must include and utilize the guiding principles of current DoD C&A guidance.

b. The USU Cyber Security Program Office shall ensure that all planning activities are scheduled and maintained to ensure USU ISs that require C&A are managed effectively. The registration and management of ports, protocols, and services shall also be addressed as part of the C&A process. Upon recommendation from their respective Certification Authorities (CAs), the Designated Approving Authorities (DAAs) shall authorize, via letter to the USU IS Program Managers (PM), an Interim Approval To Operate (IATO) for a maximum period of one year (if required), or an Approval To Operate (ATO) for a maximum period of three years. A Certification Authority/Certifier shall be designated by the DAA with the authority to establish and manage the organization's C&A program and to verify and validate IS security design and implementation through testing and review of IS security documentation.

c. An annual review will be performed as a part of the C&A process to review contingency plans, changes in to DoD Ports, Protocols, and Services Management, and security controls.

Approximately seven months prior to the expiration of the system's accreditation, or when significant changes occur or are projected to occur, the System Owner must request reaccreditation or an IATO. An IATO is reserved for ISs that have not been certified or accredited, and yet for operational reasons, must be deployed before completing certification or accreditation, or for accredited systems that cannot complete their recertification before their current certification expires.

4. Responsibilities.

a. The DAA shall:

1) Ensure that Cyber Security Managers, Cyber Security Officers, and System Administrators (SAs) are established in writing and are designated for all systems under their jurisdiction, and that they receive the level of training and certification necessary to perform the tasks associated with their assigned responsibilities.

2) Ensure the reaccreditation of ISs and networks at least every three years, or whenever previously accredited systems undergo major modifications.

3) Approve or deny IATOs in a timely manner so as not to delay operational requirements.

4) Verify that an appropriate mission assurance category has been assigned for each IS/network under his/her jurisdiction.

b. Cyber Security Officer:

1) Provide resources to perform C&A of systems, applications, and networks under their control throughout the life cycle.

2) Utilize guidance specified in USU C&A standard operating procedures and detailed instructions in references (a), through (d) in section 7.

3) Ensure C&A is accomplished prior to deployment of newly developed ISs and/or networks.

4) Ensure risk assessment is performed as part of C&A.

5) Request an IATO as soon as the security evaluation determines the need.

6) Maintain ISs security controls to comply with current DoD Cyber Security policies and directives.

7) Identify security deficiencies and take action to achieve an acceptable security level.

8) Verify data ownership, accountability, and access rights, and ensure all special handling requirements are established for each IS/network under his/her jurisdiction.

9) Ensure that all Health Insurance Portability and Accountability Act (HIPAA) Security requirements are met in accordance with reference (c) for all ISs/networks that process, store, transmit, or access protected heath information (PHI/PII).

10) Ensure processes for reporting security incidents and lessons learned are established.

11) Ensure that security safeguards approved during accreditation are implemented and maintained as necessary throughout the system life cycle.

12) Ensure that a Cyber Security awareness, training, and education program is implemented for all users, to include developers, SAs, operators, and managers.

13) Document Memorandums of Agreement (MOAs) and Memorandums of Understanding (MOUs) to address security requirements between ISs that interface or are networked and managed by different DAAs.

14) Document MOAs and MOUs to address security requirements between ISs that are interfaced or networked to non-DoD entities. If these connections process PHI/PII, then appropriate Business Associate Agreements addressing HIPAA Security requirements must also be in place.

15) Software (operation system or applications) additions, changes, or upgrades providing security features (e.g., additional functional and capability modules).

c. The Certification Authority/Certifier shall:

1) Establish and manage C&A program.

2) Ensure verification and validation IS security design and implementation through testing and review of the IS security documentation.

3) Review contingency plans and security controls on annual basis, or when significant changes occur.

4) Prepare C&A report with system certification recommendations for the DAA.

An annual review will be performed as a part of the C&A process to review contingency plans and security controls. Approximately seven months prior to the expiration of the system's accreditation, or when significant changes occur or are projected to occur, the System Owner must request reaccreditation or an IATO. An IATO is reserved for ISs that have not been certified or accredited, and yet for operational reasons, must be deployed before completing certification or accreditation, or for accredited systems that cannot complete their recertification before their current certification expires.

5. Cyber Security Requirement

Cyber Security requirements shall be established for all USU ISs. Security requirements shall consist of, but are not limited to, administrative, personnel, physical, environmental, and technical controls which shield the IS against sabotage, tampering, denial of service, espionage, fraud, misappropriation, misuse, modification, destruction, and data disclosure. The security requirements shall be satisfied through a combination of administrative, automated, and manual means in a cost-effective and integrated fashion. All USU ISs shall be evaluated to ensure minimum security standards are implemented and enforced in accordance with references *(a)* through *(d)* in section 7.

6. Reaccreditation.

a. In accordance with current DoD C&A procedures, ISs shall be reaccredited every three-years, or sooner if a significant change to hardware, software, or environment occurs. The following is a list of events affecting security that may require ISs to be recertified and reaccredited:

1) Level of criticality and/or sensitivity change for the system/environment impacting reliable baseline countermeasures.

2) Hardware additions, changes, or upgrades requiring a change in the approved security countermeasures.

3) Software (operating system or applications) additions, changes, or upgrades (e.g., additional functional and capability modules).

4) Security policy (e.g., access control policy) changes.

5) Threat change creating system vulnerability resulting in a higher risk.

6) Mission changes requiring a different security mode of operation.

7) Breaches of security, system integrity, or unusual situations that appear to invalidate the accreditation by revealing flaws in security design exposing its vulnerability.

8) Significant changes in the physical structure of the facility or the system is moved to a different facility.

9) Significant changes in operating procedures.

10) System configuration changes (e.g., a workstation connected outside of the approved accreditation parameters).

11) Networks - Inclusion of additional (separately accredited) system(s) affecting the security of that system.

12) Networks - Modification/replacement of a subscribing system affecting the security of that system.

a) Results of an audit or external analysis.

b) Addition of system interfaces with other systems.

7. References.

a. DoDI 8500.1, "Cyber Security," March 14, 2014

b. Federal Information Security Management Act of 2002

c. Public Law 104-191, "Health Insurance Portability and Accountability Act of 1996," August 21, 1996

d. CNSSI No. 4009, "National Cyber Security Glossary," May 2003

8. Revision History.

CHANGE / REVISION RECORD			
Date	**Page/Paragraph**	**Description of Change**	**Made By:**
May 2014		Review	jrobertson

Universal Serial Bus (USB) Storage Drives/Removable Devices/Media Policy

1. Purpose.

The purpose of this policy is to establish standards for the baseline configuration of all removable devices that are owned and/or operated by the USU Network Operations and Communications (NOC), users, and external system administrators (SAs) from program offices. Effective implementation of this policy will minimize data leak, the spread of malicious code, and unauthorized access to USU Information Systems (IS). It also outlines the procedures for USB storage drives (i.e., thumb drives, memory sticks, flash memory cards, hard drives etc.,) and removable devices/media (i.e., floppy diskettes/ drives, CD-ROMs /drives, DVD ROM/drives, etc.,) used on computer equipment connected to the USU network.

2. Scope.

This policy applies to all faculty, staff, civilians, and contractors who utilize the USU IS resources.

3. Policy.

a. The USB storage drives and/removable storage devices and media must be Government purchased, Government property, and be for Government use. Personal USB drives and media are not authorized for use on Government equipment.

b. The USB drive must be formatted to New Technology File System (NTFS) format rather than File Allocation Table (FAT) format.

c. Attached storage devices using USB ports with external power adapter must be powered on, at least 60 seconds prior to connecting to the network.

d. It is strongly recommended the USB drive be password protected in case of loss or theft.

e. The Government purchased USB drive must not be connected to privately-owned equipment.

f. The USB drive must be marked and protected according to the level of classification and sensitivity of the data stored on that media. Sensitive, mission-critical, and classified information requires protection from disclosure, alteration, and loss. While security requirements for information processed and stored electronically are no different from hard-copy (paper) requirements, information systems and storage media create a unique environment resulting in unique protection measures.

g. Unclassified Drives: The USB storage drive must be marked with the SF 710 unclassified labels. If the device is too small for the label, cut the label to fit the device.

h. The Cyber Security Officer, SA, and user must ensure that MP3 players, camcorders, or digital cameras are not attached to ISs without prior DAA approval.

i. The Cyber Security Officer or SA must ensure that no USB device is attached to a USU IS unless approved by the Cyber Security Officer.

j. The Cyber Security Officer, SA, and user must ensure disguised jump drives are not permitted in locations containing USU ISs.

k. The Cyber Security Officer must ensure that prominently displayed notices informing everyone of the ban of disguised jump drives, is present at all entrances of locations containing USU ISs.

l. The Cyber Security Officer, SA, and user must ensure that persistent memory USB devices are treated as removable media and in accordance with DoDM 5200.1; the devices are secured, transported, and sanitized in a manner appropriate for the classification level of the data they contain.

m. The Cyber Security Officer, SA, and user must ensure that the labeling of persistent memory USB devices is in accordance with the classification level of the data they contain.

n. The Cyber Security Officer, SA, and user must ensure that all sensitive data stored on a USB device with persistent memory, if required by the data owner, is encrypted using NIST-certified cryptography.

o. The Cyber Security Officer, SA, and user must ensure that USB devices with persistent memory are formatted in a manner to allow the application of Access Controls to files or data stored on the device.

p. The Cyber Security Officer must ensure that there is the correct usage and handling of USB technologies.

q. The Cyber Security Officer or SA must ensure that no IS has its BIOS set to allow a boot from any USB device.

r. Classified Drives:

1) If the USB storage drive is used on a classified system, it must be marked with the appropriate security classification label, secured appropriately, and included in the accreditation of the machine. It cannot be downgraded to a lower classification and must not be used on any other equipment other than for what it is classified. Classified systems and media must be labeled with the highest classification processed. SF 707 (SECRET) must be used if the classification is SECRET. If the device is too small for the label, cut the label to fit the device. Additionally, SF 712 (SCI) must be used on Sensitive Compartmented Information systems.

2) If information is downloaded to a USB storage drive, courier orders are required if the information is to leave the secure area and in a locked container to transport the classified drive.

3) If the drive is not hand carried, it must be transported by a designated person in the Defense Courier Service and properly wrapped, stamped, and enclosed in a GSA- approved pouch or container if leaving a secure area and going off-site.

4) If a device containing classified information is lost or stolen, the user's Cyber Security Manager and NOC Director must be notified immediately. The Cyber Security Manager can assign an investigator to implement an investigation to assess the damage and determine necessary procedures to mitigate the risk.

5) Devices cannot be purged or released outside DoD control. At the end-of-life cycle, the device must be destroyed.

4. Responsibilities.

a. Personnel are reminded that violations of these policies may be punishable under the Uniform Code of Military Justice and/or United States Code.

5. References.

a. DoDI 8500.01, "Cyber Security," March 14, 2014

b. DoDI 8500.2, "Cyber Security Implementation," February 6, 2003

c. "Military Health System Cyber Security Policy/Guidance Manual," February 12, 2003 (hereby canceled)

d. DoDI 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014

SYSTEM LIFE CYCLE MANAGEMENT

1. Purpose.

The USU Cyber Security System Life Cycle Management (LCM) process ensures required security safeguards are developed and executed to protect ISs against accidental or intentional unauthorized modification, disclosure, destruction, and denial of service throughout the life cycle of the system. Including security early in the IS development life cycle, rather than adding it to an operational system, will usually result in less expensive and more effective security.

2. Scope.

This policy applies to all USU users to include faculty, staff, students, guests, contractors and volunteers that utilize, plan, and/or manage USU IS resources.

3. Policy.

It is USU Policy that:

a. Cyber Security requirements be identified and included in the design, acquisition, installation, operation, and upgrade or replacement of USU ISs.

b. Required Controls are implemented to protect USU ISs against unauthorized modification, disclosure, destruction, and denial of service throughout the security development life cycle phases.

c. As early as possible in the life cycle of IT-dependent programs, information owners shall establish the Mission Assurance Category (MAC), security classification, sensitivity, and need-to-know of information and information systems.

d. The Cyber Security controls are established as part of the baseline requirements consistent with DoDI 8500.2, "Cyber Security Implementation," February 6, 2003, and are implemented throughout the system's life cycle. DoDI 8500.2 provides a detailed list of the IA controls necessary to achieve the baseline levels of confidentiality, integrity, and availability.

e.USU Components shall, at a minimum:

1) Develop security specifications based on DoD Cyber Security Controls.

2) Identify risk areas and define risk reduction measures, management approaches, and plans.

3) Test and evaluate to certify that technical security features and other safeguards satisfy specified security requirements before the initiation of operational testing.

4) Establish procedures to ensure continuous use of approved security safeguards during the production, deployment, implementation, and operational/maintenance phases.

5) Ensure Cyber Security requirements are addressed and incorporated into the acquisition documentation in accordance with DoDI 8580.1, "Cyber Security in the Defense Acquisition System," July 9, 2004.

4. Procedures.

a. Cyber Security LCM incorporates operational requirements for security in all IS planning and design, and ensures conformance with applicable security regulations, policies, and requirements. The product of this activity is the Cyber Security Strategy. The USU Component sponsoring the system development shall have an understanding of the nature, need, and information processed by the system to determine the information's sensitivity and criticality.

1) Security System Life Cycle Management Phases.

Security planning shall be implemented throughout a system life cycle. At a minimum, USU shall incorporate the following security into the system life cycle:

a) Initiation Phase

1. Security Categorization defines the MAC level to establish the Cyber Security controls based on confidentiality levels. Designation of a MAC level assists the USU Component in identifying the appropriate security controls based on the sensitivity of the information.

2. Preliminary Risk Assessment results in the initial description of the basic security needs of the system. A preliminary risk assessment defines the threat environment in which the system will operate.

b) Acquisition/Development Phase

1. Risk Assessment – analysis that identifies the protection requirements for the system through a formal risk assessment process. This analysis builds on the initial risk assessment performed during the Initiation Phase, but is more in-depth and specific.

2. Security Functional Requirements Analysis – analysis of requirements that may include the following components: (1) system security environment (policies and architecture) and (2) security functional requirements.

3. Cyber Security Controls Analysis – analysis of Cyber Security controls that address the required development activities and the assurance evidence needed to produce the desired level of confidence in the accuracy and effectiveness of the information security. This analysis shall ultimately become part of the baseline Cyber Security requirements.

4. Cost Consideration and Reporting – determines the amount of development attributed to information security over the life cycle of the system. This cost includes hardware, software, personnel, and training.

5. System Security Authorization Agreement Planning – ensures that Cyber Security controls are planned, agreed upon, in place, and fully documented. The security plan shall also provide a complete characterization or description of the IS, as well as the attachment of references to key documents and programs supporting the IS security program (e.g., configuration management plan, contingency plan, incident response plan, Cyber Security Vulnerability Management (CSVM), security awareness and training, rules of behavior, risk assessment, security test and evaluation results, system interconnection agreements, certification and accreditation, and plan of action and milestones).

6. Cyber Security Control Development – ensures that Cyber Security controls are described in the security plans and are implemented consistent with DoD. For ISs currently in operation (e.g., legacy systems), the security plans may call for additional Cyber Security controls or modification of existing Cyber Security controls.

7. Developmental Security Test and Evaluation – ensures that Cyber Security controls chosen and developed for a new IS are working properly and effectively.

8. Other Planning Components – ensures that all components of the development process are considered when incorporating Cyber Security into the life cycle. These selections include appropriate contract type, participation by all related functional groups, participation by certifier and accreditor, and development and execution of necessary contracting plans and process.

c) Implementation Phase

1. Inspection and Acceptance – ensures that the USU Cyber Security Program Office and local Designated Approving Authority (DAA) validate and verify that the functionality described in the specification is included in the deliverables.

2. Security Control Integration – ensures that Cyber Security controls are integrated at the operational site where the IS is to be deployed for operation. Security control settings and switches are enabled in accordance with DoD directives.

3. Cyber Security Certification – ensures that the Cyber Security controls and MAC designation are effectively implemented through the DoD Cyber Security Certification and Accreditation Process (DIACAP) and appropriate safeguard measures are in place.

4. Cyber Security Accreditation – ensures the appropriate DIACAP accreditation is granted by the authorized Certification Authority and DAA based on the effectiveness of Cyber Security controls in place.

d) Operation/Maintenance

1. Configuration Management and Control – ensures adequate consideration of the potential security impacts due to specific changes to an IS or its surrounding environment. Configuration management and configuration control procedures are critical to establishing an

initial baseline of hardware, software, and firmware components for the IS, subsequently controlling and maintaining an accurate inventory of any changes of the system.

2. Continuous Monitoring and Testing – ensures that controls continue to be effective in their application through periodic, unannounced, in-depth monitoring and testing to be reported to the USU Cyber Security Program Office. This includes specific penetration testing to ensure compliance with all vulnerability mitigation procedures such as the DoD Cyber Security Vulnerability Alert (CSVA) or other DoD Cyber Security practices that are planned, scheduled, and conducted. Testing is intended to ensure that the system's Cyber Security capabilities continue to provide adequate assurance against constantly evolving threats and vulnerabilities.

e) Disposition Phase

1. Information Preservation – ensures that information is retained, as necessary, to conform to DoD sensitive information protection requirements.

2. Media Sanitization – ensures that hardware and software are disposed of in accordance with current DoD policy and the applicable USU Cyber Security policy implementation guide.

2) Cyber Security Manager (CSM) Responsibilities -- At a minimum, the CSM for acquisition programs shall:

a) Remain ultimately responsible for the platform's overall Cyber Security protection for acquisitions of platforms with internal information technology (IT), including platforms such as network operations and communication technologies.

b) Retain responsibility to incorporate all Cyber Security protective measures necessary to support the platform's support mission functions for acquisitions of platforms with IT that do not interconnect with external networks.

3) Identify all assurance measures needed to ensure both the protection of the network and the protection of the platform from connection risks, such as unauthorized access, that may be introduced from the network.

4) Demonstrate prudent judgment by considering the Cyber Security program provisions in DoDD 8500.1 and DoDI 8500.2 for systems that are not connected to external networks and that do not involve internal networks, and employing those Cyber Security controls appropriate to their system.

5) Be responsible for coordinating with enclaves that host (run) Automated Information Systems (AISs) applications early in the acquisition process to address operational security risks the system may impose upon the enclave, as well as identifying all system security needs that may be more easily addressed by enclave services than by system enhancement.

6) Comply with the Cyber Security requirements in the DoD 8500 policy series for acquisitions of outsourced IT-based processes.

7) Be responsible for employing the sets of baseline controls appropriate to their programs.

5. References.

a. ASD (C3I) Memorandum, "Disposition of Unclassified DoD Computer Hard Drives," June 4, 2001

b. Assistant Secretary of Defense (Health Affairs) Memorandum, "Military Health System Cyber Security Policy Guidance," March 5, 2004

c. DoDD 5000.1, "The Defense Acquisition System," May 12, 2003

d. DoDI 5000.2, "Operation of the Defense Acquisition System," May 12, 2013

e. DoD 5000.2-R, "Mandatory Procedures for Major Defense Acquisition Programs (MDAPS) and Major Automated Information System (MAIS) Acquisition Programs," April 5, 2002

f. DoDI 8500.01, "Cyber Security ," March 14, 2014

g. DoDI 8580.1, "Cyber Security in the Defense Acquisition System," July 9, 2004

h. Federal Information Security Management Act of 2002

i. NIST Special Publication 800-64, "Security Consideration in the Information, October 2003

j. Health Insurance Portability and Accountability Act (HIPAA) Security Final Rule, February 20, 2003

6. Revision History.

CHANGE / REVISION RECORD			
Date	**Page/Paragraph**	**Description of Change**	**Made By:**
26 Jan 2011		USU Updates	R. O'Grady

DoD Public Key Infrastructure (PKI) and Public Key Enabling (PKE)

1. Purpose and Scope.

a. The provisions of this guide are policy for all USU Component(s). For USU Contractors, this document is policy if required by contract; otherwise it serves as Cyber Security guidance.

b. Public Key Infrastructure (PKI) is a technology consisting of a system of hardware, software, policies, and people that, when fully and properly implemented, can provide a suite of information security assurances that are important in protecting sensitive communications and transactions. PKI brings to the electronic world the security and confidentiality features provided by the physical documents, hand-written signatures, sealed envelopes, and established trust relationships of traditional, paper-based transactions. These features are:

1) Confidentiality – ensures that only intended recipients can read files (sealed envelope).

2) Data Integrity – ensures that files cannot be changed without detection (hand-written signature and sealed envelope).

3) Authentication – ensures that participants in an electronic transaction are who they claim to be (hand-written signature).

4) Non-repudiation – prevents participants from denying involvement in an electronic transaction (established trust relationships and registered mail).

c. This implementation guide provides guidance for accomplishing DoD PKI/Public Key Enabling (PKE) activities within the USU and supplements that provided in reference

d. This guide is applicable to all USU Centrally Managed ISs and networks and ISs and networks developed and operated by DHA, including contracted services.

2. Policy.

USU shall follow current DoD PKI and PKE policy. Current DoD PKI/PKE policies may be newer than the references contained in this guide.

3. Procedures.

a. Cyber Security Manager is responsible for:

1) Ensuring DoD PKI/PKE requirements for private web servers are met. Procedures include:

a) Identifying DoD private web servers under their cognizance.

b) Requesting, installing, and maintaining the DoD PKI server certificate, and enabling its use to identify the server and to protect the transmissions between the server and the client's browser.

c) Ensuring that DoD certificates are used for their intended web server and are not placed on any other server or system.

d) Relying on DoD-approved PKI certificates for client authentication to the DoD private Web server per DoD PKI/PKE policy. PKI user authentication includes validating that the certificate is from a trusted source, has not expired, or has not been revoked.

e) Providing a transition period for web server users to be able to move from the current authentication method to use of PKI.

f) Ensuring DoD PKI requirements are included in contracts and met by the contractor.

g) Ensuring DoD PKI is employed when the application requires a service that DoD PKI supports (e.g., strong authentication, digital signature, and data integrity).

h) Verifying application/system compatibility with DoD PKI by conducting interoperability and compatibility testing except for commercial off-the-shelf (COTS) products already tested by DoD or a Component.

i) Ensuring that applications and systems that are PK-enabled as a result of a BCA meet the DoD policy requirements for PKI and PKE, and these are met by the DoD-set milestone dates. Lack of time, planning, or resources are usually not an acceptable justification for missing a milestone date.

b. Network Operations and Communications (NOC) Network and Operations managers are responsible for:

1) Enabling the USU network to rely on DoD-approved PKI certificates contained on a DoD approved hardware token (e.g., Common Access Card (CAC)) for user authentication and access control to the network per DoD PKI/PKE policy. PKI user authentication includes validating that the certificate is from a trusted source, has not expired, and has not been revoked.

2) Verifying network-provided application/system compatibility with DoD PKI by conducting interoperability and compatibility testing except for COTS products already tested by DoD or a Component.

3) Ensuring e-mail, including web-based e-mail, is capable of using DoD PKI certificates for digital signature and encryption. This includes relying on DoD-approved PKI certificates for user authentication to the e-mail private web server.

4) Ensuring network workstations and network provided remote access laptops have CAC readers and middleware installed to support PKI per DoD PKI/PKE policy.

5) Providing personnel training on the correct use and protection of the PKI certificate.

6) Incorporating PKI into the network's security documents and having them available for DoD Cyber Security Certification and Accreditation Program (DIACAP) reviews, such as procedures and guidance for handling access to the network when a PKI certificate is not available for a user including priority and emergency access.

c. USU users of PKI are responsible for:

1) Using their DoD PKI certificate for DoD business only. Protecting their PKI certificates.

a) An individual's certificate or Personal Identification Number (PIN) shall not be shared, regardless of certificate storage method or location.

b) Maintaining control of the PKI certificate token at all times. If the PKI certificate is stored on a hardware token (CAC), the user must remove it from the workstation and take the CAC with them whenever they leave the immediate area of the workstation.

c) Protecting the PIN used to access the user's PKI certificates as they would any password (e.g., memorize the PIN and not write it down or post on terminals or blackboards; do not tell any other user or person what the PIN is).

2) Reporting to a CAC PIN reset facility as soon as possible after three consecutive unsuccessful attempts at entering the correct PIN locks the CAC.

a) Users of the USU network should contact the USU Security Department for CAC PIN reset.

b) USU network users not located on or near the main USU campus, should contact their Service's local command Cyber Security or network security official for the location of the nearest CAC PIN reset facility.

3) Reporting to the immediate supervisor and designated office, as soon as possible upon recognizing that the event has occurred, any lost, missing, stolen, or compromised PKI certificates including a certificate PIN, whether stored on soft or hardware tokens.

a) For users of the USU network, the designated office for reporting lost, missing, stolen, or compromised PKI certificates on CACs is the USU Security Department.

b) For users of the USU network not located on or near the main USU campus, the designated office for reporting lost, missing, or stolen PKI software certificates is the HA/DHA network Local Registration Authority (LRA) who issued their certificate.

c) For users not on the USU network, the designated office is provided by the Service's local command Cyber Security guidance or network security guidance. At a minimum, the user should report the event to their supervisor and the local network security officer.

d) Users who suspect that the PIN has been compromised must go to the CAC PIN reset facility and have the PIN changed.

4) Obtaining a replacement PKI certificate for any lost, missing, stolen, compromised, or expired certificate/token.

a) This includes resubmitting any required forms with signatures for approval in accordance with local guidance. A DD1172 form is required for a CAC.

b) For PKI certificates stored on DoD CACs, this involves traveling to a CAC issuance facility to obtain a replacement.

5) Following DoD PKI policy and Service/organization-specific guidance for when one should apply the user's PKI certificate for digitally signing and encrypting e-mail or digitally signing a document.

a) Must use digital signatures when sending e-mails to outside organizations that include official correspondence or hyperlinks.

b) Emails must be encrypted when sending sensitive information in e-mail.

c) Following the application Cyber Security and PKI guidance and procedures to apply the user's PKI certificate for a transaction or data in an application.

d. Contractors accessing DoD networks or systems or doing electronic business with DoD from their own networks are responsible for:

1) Using only DoD-approved certificates from an authorized DoD External Certificate Authority (ECA) when conducting electronic business that requires PKI with DoD.

a) Specific guidance requiring the use of DoD PKI shall be provided in contractual documents and correspondence.

b) Information on the DoD ECA program, including how to purchase DoD-approved ECA PKI certificates can be found at http://iase.disa.mil/pki/eca/index.html.

c) DoD-approved ECA certificates are different from standard PKI certificates from vendors.

2) Using DoD PKI ECA certificates only for authorized DoD business unless authorized by DoD for use with other DoD partners (Federal, state, local governments, or contractors).

3) Contractors shall establish Cyber Security guidance and procedures for controlling DoD ECA PKI certificates and have them available for DIACAP reviews. These should at a minimum include:

a) Identifying personnel whose job function requires a DoD ECA PKI certificate

b) Authorizing and purchasing a DoD-approved PKI certificate from a DoD ECA.

c) Tracking who is issued certificates, when issued, job function requiring PKI certificate, date of revocation, and reason for revocation.

d) Providing personnel training on the correct use of the PKI certificate.

e) Providing rules for their use (signing e-mail, access to DoD networks or systems, etc.), protection of the PIN, renewal, and handling compromise and revocation including loss or no longer required (job change, departure from company, etc.).

f) Assigning responsibilities for PKI management, ensuring technical matters are properly handled including removing certificates when no longer required or are revoked.

4) Ensuring that DoD ECA certificates are not shared or used by anyone except the specific individual for whom the ECA authorized and provided the certificate.

5) Ensuring that any compromised or no longer required certificate is reported in accordance with the ECA guidance and procedures where the certificate was purchased.

4. References.

a. DoD Instruction 8520.2 "Public Key Infrastructure (PKI) and Public Key (PK) Enabling," April 1, 2004

b. Assistant Secretary of Defense (HA) Memorandum, "Military Health System Cyber Security Policy Guidance," March 5, 2004

c. DoD Chief Information Officer (CIO) Memorandum "Public Key Infrastructure (PKI) and Public Key Enabling (PKE)," October 7, 2003

d. DoD Under Secretary of Defense for Personnel and Readiness Memorandum, "Common Access Card Issuance Mandate," September 25, 2003

e. DoD Directive 8190.3, "Smart Card Technology," August 31, 2002

f. Assistant Secretary of Defense Memorandum, "Guidance and Provisions for Developing Department of Defense (DoD) Component's Public Key Enabling (PKE) Policy Compliance Waiver Process," August 5, 2002

g. Assistant Secretary of Defense Memorandum, "Public Key Infrastructure (PKI) Policy Update," May 21, 2002

h. DoD CIO Memorandum, "Public Key Enabling (PKE) of Applications, Web Servers, and Networks for the Department of Defense (DoD)," May 17, 2001

i. DoD CIO Memorandum, "Common Access Card," January 16, 2001

j. DoD CIO Memorandum, "Department of Defense (DoD) Public Key Infrastructure (PKI)," August 12, 2000

k. DEPSECDEF Memorandum, "Smart Card Adoption and Implementation," November 10, 1999

l. DoDI 5230.29, "Security and Policy Review of DoD information for Public Release," August 6, 1999

m. DoDD 5230.9, "Clearance of DoD Information for Public Release," April 9, 1996

n. Federal Information Security Management Act of 2002

5. Definitions.

Common Access Card – A Department-wide smart card used as the standard identification card for active duty Uniformed Services personnel (to include the Selected Reserve), DoD civilian employees, eligible contractor personnel, and eligible foreign nationals; the primary platform for the public key infrastructure authentication token used to access DoD computer networks and systems in the unclassified environment and, where authorized by governing security directives, the classified environment; and the principal card enabling physical access to buildings, facilities, installations, and controlled spaces as described in DoDD 8190.3, "Smart Card Technology," dated August 31, 2002.

DoD Private Web Server (From DoDI 8520.2, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling," dated April 1, 2004) – For unclassified networks, a DoD private web server is any DoD-owned, operated, or controlled web server providing access to official information that has not been reviewed and approved for release in accordance with DoDD 5230.9 and DoDI 5230.29. For Secret Internet Protocol Router Network and other classified networks that are not accessible to the public, a DoD private web server is any server that provides access to information that requires need-to-know control or compartmentation.

Token (From DoDI 8520.2) – A portable, user-controlled, physical device used to generate, store, and protect cryptographic information, and perform cryptographic functions.

6. Revision History.

CHANGE / REVISION RECORD			
Date	**Page/Paragraph**	**Description of Change**	**Made By:**

CYBER SECURITY VULNERABILITY MANAGEMENT (CSVM) PROGRAM

1. Purpose.

This policy establishes the USU CSVM program and provides responsive and effective vulnerability management as required by Chairman of the Joint Chief of Staff Manual (CJCSM) 6510.01, "Computer Network Defense." This policy also establishes responsibilities and procedures for the CSVM program, to include organizational and individual responsibilities, registration, compliance criteria, extensions, enforcement, and verification.

2. Scope.

This policy applies to all USU employees to include contractors that use, manage, plan, and implement USU IT resources.

3. Policy.

It is USU policy that System Administrators (SAs) must monitor and report mitigation of known Cyber Security Vulnerability Alerts to the USU CSVM Monitor through the DoD Vulnerability Management System (VMS).

4. Procedures.

a The Cyber Security Manager must:

1). Designate a primary and secondary representative responsible for managing its internal CSVM program and register primary and secondary POCs in the VMS.

2). Acknowledge receipt of the IAVA or IAVB messages within five days of release.

3). Ensure vulnerability messages are disseminated to all appropriate SAs within the USU, to include but not limited to program managers, Cyber Security Officers, System Administrators (SAs), and/or other personnel responsible for implementing and managing responses to IS vulnerabilities.

4). Ensure all subordinate organizations comply with all Cyber Security Vulnerability Alerts within the designated compliance window or in accordance with the extension process.

5). Report IAVA compliance status via VMS as specified in the individual IAVA message (typically 30 days from the date on the message) and update the VMS weekly, at a minimum.

6). Review second and third extensions and their associated mitigation plans and implementation timelines. This role will be filled by the Designated Approving Authority (DAA) unless delegated to the USU CIO.

7). Establish a process to ensure that all DoD contracts for DoD ISs and services contain language requiring participation in the CSVM program.

8). Conduct CSVM program compliance checks of their subordinate organizations.

b. Roles & Responsibilities.

1). The DAA must:

a). Order the affected assets disconnected from the network if unable to submit an action plan describing steps to be taken to achieve compliance with outstanding Cyber Security Vulnerability Alerts.

b). Review extension requests and, if appropriate, disconnect compromised systems from the network immediately.

c). Review and, if appropriate, approve the first 30-day extension (local DAA) that would allow continued operation of the non-compliant system.

2). The Cyber Security Manager must:

a). Ensure IAVA notices are disseminated to the lowest level Cyber Security Officer, SAs, and other individuals identified as participants in the CSVM process.

b). Ensure all subordinate organizations comply with all Cyber Security Vulnerability Alerts within designated compliance window or in accordance with the extension process.

c). Monitor IAVBs and TAs.

d). Review requests for extensions; monitor extension plans with their associated mitigation plans and implementation timelines as required.

e). Ensure that all required risk mitigation actions are implemented in accordance with associated timeline if extension to an IAVA is granted.

f). Ensure compliance checks of their subordinate organizations to make certain mitigating and/or corrective actions are completed.

g). Review approved mitigation action plan and include it as part of an extension request.

3). Programs centrally managed at the USU level or at the USU Enterprise level must establish a capability to effectively mitigate the risk posed by critical vulnerabilities as identified in IAVA notices. Joint or Enterprise-wide Program Managers must:

a). Register with the VMS for a User Identification (ID) and password for VMS.

b). Designate a primary and secondary CSVM POC.

c). Respond to each CSVM message as the system configuration manager.

d). Acknowledge receipt of the CSVM messages through VMS.

e). Publish a program action plan for every CSVM notice issued by DoD CERT; the program plan should provide an initial status.

f). Provide periodic status updates, as required, throughout the life cycle of the vulnerability until the corrective action has been completed.

g). Ensure dissemination of the action plan, if necessary, to affected SAs.

h). Process program level extensions through the appropriate program DAA.

4). The Cyber Security Office must:

a) Maintain positive configuration control of all ISs and/or assets under their purview. Maintain configuration documentation that identifies specific system and/or asset owners and SAs including applicable network addresses.

b). Ensure networked assets are managed and administered in a manner allowing both chain of command and authorized independent verification of corrective actions.

5). Designated CSVM representatives must:

a). Register with the MHS CSVM Monitor for assignment of User ID and password in the VMS system.

b). Disseminate IAVA notices to lowest level SAs.

c). Enter their organization's acknowledgment and compliance and/or extension data into VMS/Vulnerability Compliance Tracking System (VMS/VCTS).

d). Monitor compliance status for CSVM Alerts, and update VMS as statistics change throughout the life cycle of the IAVA.

e). Prepare, review, and forward requests for extensions. Extensions should be passed along to the DAA for further review and adjudication.

6). The SA must:

a). Ensure all devices are IAVA compliant prior to connecting the devices to DoD networks.

b). Respond to all active Cyber Security Vulnerability Alerts – any asset found with an active vulnerability, where the IAVA completion date has closed, must be brought into compliance immediately, have an extension request submitted, or the asset must be disconnected.

c). Test and evaluate all patches intended to resolve an IAVA and obtain permission from the Project Officer before deploying the fix to a device. An extension should be requested if the supplied fix is unsatisfactory and another fix must be researched or developed.

d). Monitor for new vulnerability notices.

e). Report compliance and/or extension information through the command channels for aggregation and reporting.

f). Prepare and submit an extension and mitigation action plan (including implementation timelines) within the time specified in the IAVA notification message (usually 30 days), if unable to comply with an IAVA.

c. IAVA Extensions and Compliance Process and Timelines

1). The extension process has been broken into three categories (First, Second, and Third Extensions).

a). The FIRST extension begins the day after the original compliance window identified in the IAVA notification message closes and runs for up to 30 days (Note: The normal compliance window is 30 days, but may be adjusted by the USCYBERCOM).

b). The SECOND extension begins the day after the first extension ends and runs for 60 days.

c). The THIRD extension begins the day after the second extension ends and runs for a period directed by the approval authority, for a maximum of two years.

2). Extension approval authority is determined by the extension category being requested. Once extensions are approved, VMS must be updated to reflect the approval. The database must also be updated when the extension has been closed.

3). First extensions are approved by the local DAA. Approval of this first extension authorizes the system to operate for 30 additional days while mitigation actions are implemented to reduce risk. Extension requests must include:

a). System being addressed.

b). Name of system.

c). Description of system, including media access control (short paragraph).

d). Internet Protocol address and machine name (if applicable).

e). Media Access Control address (if applicable).

f). IAVA number.

g). Date of the request.

h). Estimated date of completion.

i). Reason for extension.

j). A Plan of Action (POA) describing in detail what steps will be taken to test and apply an appropriate patch for the vulnerability described within the IAVA.

k). A series of milestones indicated within the POA that provide a specific timeline for remedy actions.

l). A risk assessment of high, medium, or low risk. Risk assessment should consider, as a minimum, the number of systems affected, indications and warnings, mitigation plans and/or actions, and potential operational impact of non-compliance.

m). Identification of the approving DAA.

n). POC (Name, e-mail address, telephone number).

o). Approval must be based on a sound extension plan with mitigation actions that minimize the risk of compromise to local systems. Local DAAs must consider the associated risk shared by other DoD networks when approving an extension.

4). The USU DAA approves second extensions. Approval of this second extension allows the asset to operate for 60 additional days while mitigating activities are performed.

a). Any additional mitigation actions required to protect assets during the second extension period must be provided along with a strong justification for extension.

b). The USU DAA approves third extensions. Third extensions are reserved for rare cases where circumstances have prevented compliance with an IAVA during the timelines for first or second extension, to include mission required legacy systems that cannot meet IAVA requirements. The extension packages must be revalidated, including the latest extension plan, timeline, and proposed mitigation actions.

5). Third extension mitigation plan must include:

a). Mitigating policies, processes, and procedures that have been implemented (e.g., actions that have been prohibited or controlled or monitoring processes that have been employed or intensified).

b). Network-level actions, to include use of security tools such as firewalls, security routers, proxy devices, and intrusion detection systems (IDSs

c). Server-level actions to limit attachment size on exchange servers.

d). Any system-level actions, such as disabling services, host level firewalls, and IDSs, as necessary.

e). A statement that a vulnerability assessment, evaluating the effectiveness of the mitigating actions, has been conducted of the vulnerable system; a copy of vulnerability assessment must be available for review.

f). A statement of milestones and end date for accomplishing the IAVA implementation. Open third extensions must be reviewed and revalidated by the USU CIO at least annually, and VMS must be updated to reflect the outcome of the review. The database must be updated when the extension has been closed.

d. VMS User Enrollment and Training

All users assigned responsibility to update or monitor CSVM compliance in VMS must apply for and obtain a VMS account. The USU CSVM Coordinator must create VMS accounts and assign appropriate permissions, or allow heads of Program Offices to assign permissions to their subordinate users. Individuals who wish to apply for an account within VMS should complete a DD Form 2875, "System Authorization Access Request (SAAR)", May 2004, available from DISA, and return the completed form to the USU CSVM Coordinator for review and approval by USU IA Branch. Applicants should contact the USU CSVM Coordinator to obtain guidance on how to properly complete the DD Form 2875 before submitting their form.

Applicants should meet the minimum qualifications prior to applying for a VMS account:

1). For U.S. citizens: Possess a NAC or better investigation, and accompanying interim or final investigation or designation.

2). For non-U.S. citizens: Possess a final Secret clearance, or a final ADP/IT-I, II, or III designation.

Training is available through DISA and within the VMS application. New VMS users should review the training module available within the VMS application, or contact DISA for live training.

Interim Access: Upon completion and submission of appropriate paperwork, interim access may be granted. Interim access is granted only to US citizens.

e. Component Non-Compliance Notification and Enforcement Procedures

1). Commander, USCYBERCOM, must notify non-compliant DoD component IAVA authority POC to verify IS or network is non-compliant and to coordinate a resolution.

2). DoD components must be considered non-compliant under any of the following conditions:

DoD organization has not acted to update IAVA status within directed compliance window.

a) Non-compliant computer assets operating without approved extension and mitigation plan.

b) If USU is not responsive or fails to follow through with resolving the non-compliance, USCYBERCOM must release an IAVA non-compliance message addressed to the USU CIO.

3). Non-compliant DoD components must be requested to respond within 72 hours with reasons for non-compliance, planned corrective actions, mitigation plan, and operational impact; DoD components must respond to USCYBERCOM.

4). USCYBERCOM must review planned component corrective actions and coordinate any additional actions required to mitigate vulnerability created by non-compliance in accordance with Paragraph 5.12.5, DoDI 8530.1, "Computer Network Defense", January 8, 2001.

a) USCYBERCOM, in coordination with the Joint Staff (J-3 and J-6), must determine global operational impact of continued IAVA noncompliance as required.

b) If USCYBERCOM or a DoD component has an issue that cannot be resolved concerning compliance actions, Assistant Secretary of Defense (Networks & Information Integration) (ASD (NII)) and the Chairman of the Joint Chiefs of Staff must be informed.

5. References.

a. DoDI 8500.01, "Cyber Security," March 14, 2014

b. CJCSM 6510.01, Change 1, "Defense in Depth: Cyber Security and Computer Network Defense," August 10, 2004

c. DoDI 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014

d. DoDI 853.1, "Computer Network Defense", January 8, 2001.

f. DoDI 8530.2, "Support to Computer Network Defense (CND)," March 9, 2001

g. DoDM 5200.1, "Information Security Program," February 24, 2012

h. DoDI 5200.2-R, Change 3, "Personnel Security Program," February 23, 1996

i. Federal Information Security Management Act of 2002

j. Health Insurance Portability and Accountability Act (HIPAA) Security Final Rule, February 20, 2003.

6. Revision History.

CHANGE / REVISION RECORD			
Date	**Page/Paragraph**	**Description of Change**	**Made By:**

Security Education, Training and Awareness

1. References.

a. DoDI 8500.01, "Cyber Security," March 14, 2014

2. Purpose.

This policy provides guidance on the training requirements for System Administrators (SA), Network Administrators (NA), and end users of the USU IS.

This document establishes guidance and assigns the roles and responsibilities needed to ensure that sufficient Cyber Security and technical training is provided within the USU to comply with DoD policies and best business practices. Adherence to the provisions in this guidance ensures that an appropriate and consistent level of security awareness is achieved in order to maintain availability, integrity, authentication, confidentiality, and non-repudiation of the USU IS.

This guidance directly supports the mission of the USU by applying the principles of DoD IT management. This includes developing and implementing policies, procedures, programs, and technical standards necessary to acquire, manage, integrate, and secure information technology systems and capabilities that support the USU teaching and research mission.

3. Applicability.

USU recognizes that technology is evolving at a rapid rate and understands the need for personnel to develop skills to keep pace with technology changes. Therefore, a training program must be developed which ensures that USU retains qualified staff to administer the USU IS and maintain an IA program.

a. Cyber Security training is an integral part of ensuring that USU resources are effectively secured and protected from internal and external breaches and exploitations.

b. This policy provides directives for the establishment and on-going involvement of an IA training program for USU network/system administrators, end-users, and IA personnel.

c. USU designs, implements, operates, and maintains information technology and local and wide area communications infrastructure that supports several user groups within the University. Various IA personnel and network/system administrators and managers are responsible for operating, maintaining, and safeguarding these information resources. It is crucial that these personnel are adept in the security measures and safeguards that must be used and implemented in order to provide for continuous protection of USU assets. The end-user community must also be aware of the various security vulnerabilities associated with automated information systems (AIS) and USU information resources. In order to sustain a steadfast security posture, end-users must know what precautions to take to maintain the security posture and how to recognize possible exploits and breaches and report these threats if they occur.

d. This policy applies to all faculty, staff, civilians, and contractors, who plan, deploy, configure, operate, or maintain resources or services in connection with the USU IS.

4. Responsibilities.

a. Compliance with this policy is the responsibility of the respective business unit manager\director.

b. The USU Cyber Security Manager provides oversight and verification of compliance with all USU IA training requirements for IA staff, network and system administrators, and end-users.

c. USU personnel are responsible for identifying opportunities and requesting approval for training from respective providers (e.g., SANS conference, Microsoft certification training, Cisco training, etc.) that would enhance their professional and technical qualifications and provide direct or ancillary benefit to their primary duties and responsibilities. Each individual must seek approval for such training through his or her normal chain of command. Individuals completing a training course must submit a notification of completed training to the Cyber Security Manager and the USU Training Coordinator.

5. Policy.

a. All network administrators, system administrators, and Cyber Security personnel, to include the Cyber Security Officer and the Cyber Security Manager, must complete a course of instruction equal to the duties assigned to them, in which the course includes an IA component.

1) Each cell within Table 1-1 provides a list of DoD-approved certifications personnel performing IA functions may use to meet baseline requirements. The Cyber Security Manager will utilize this list to determine IA certification training requirement for USU personnel performing in each of the IAT levels.

Cyber Security Technical (IAT) Workforce		
IAT Level 1	**IAT Level II**	**IAT Level III**
A+ Network + SSCP	GSEC Security + SSCP	CISA CISSP (or Associate) GSE SCNA
Cyber Security Management (IAM) Workforce		
IAM Level I	**IAM Level II**	**IAM Level III**
GISF GSL C	GSL C CISM	GSL C CISM

Computer Network Defense (CND) Workforce				
CND Analyst	**CND Infrastructure Support**	**CND Incident Responder**	**CND Auditor**	**CND Service Provider (SP) Manager**
GCI A CEH	SSC P CEH	GCIH CSIH CEH	CISA GSN A	CISSP- ISSMP CISM

Cyber Security System Architecture and Engineering (IASAE) Workforce		
IASAE I	**IASAE II**	**IASAE III**
CISSP (or Associate)	CISSP (or Associate)	ISSE P

Table 1-1: DoD-Approved Baseline Certifications

2) A record of completed training for Cyber Security personnel must be filed with the Cyber Security Manager and the USU Training Coordinator.

a) The USU Cyber Security Manager must oversee the development of an Information Security Awareness Training Module that is computer based and can be completed within 30 minutes by an end user with average IT skills. The Information Security Awareness Training Module must be updated as technology and security issues change and develop.

1. All USU end-users must undergo an initial security training and Cyber Security awareness briefing upon reporting to USU. The briefing must include the following: threats, vulnerabilities, and risks associated with the system. Under this portion, specific information regarding measures to reduce the threat from malicious software will be provided, including prohibitions on loading unauthorized software, the need for frequent backup, and the requirement to report abnormal program behavior immediately.

2. Information security objectives, such as what is it that needs to be protected.

3. Responsibilities and accountability associated with system security.

4. Information accessibility, handling, and storage considerations.

5. Physical and environmental considerations that are necessary to protect a system.

6. System data and access controls.

7. Emergency and disaster plans.

8. Authorized system configurations and associated configuration management requirements.

9. Refresher training will be completed on an annual basis

6. Revision History.

CHANGE / REVISION RECORD			
Date	**Page/Paragraph**	**Description of Change**	**Made By:**

USU Password Policy

1. Purpose.

The purpose of this policy is to establish standards for the baseline configuration of passwords on all devices that are owned and/or operated by USU Network Operations and Communications (NOC), external System Administrators (SAs), and End Users. Effective implementation of this policy will minimize mis-configurations and unauthorized access to USU information systems (ISs).

2. Scope.

This policy applies to all USU IS whether connected to the network or stand alone.

3. Policy.

a. Password Length and Composition: All passwords must be 15-characters in length to include accounts with administrator, root, or super user privileges. Passwords must contain a mix of at least two lowercase letters, two uppercase letters, two numbers, and two special characters (i.e.,!@#$%^&*?). Care should be taken to avoid use of sequential characters, or keyboard walks, when formulating passwords. Management accounts for applications/functions are considered similar to admin/root/super-user accounts, and hence must also implement 15-character passwords. For those operating systems that do not support 15-character passwords (such as UNIX), employ the full length of the password character string allowable and the strongest combination of lower, upper, number, and special characters.

b. Initial Password Assignment: The System Administrator is responsible for generating and assigning the initial temporary password for each new user ID. The new user is then forced to change the temporary password at initial logon.

c. Nullifying Exposure: Each user must present their Government ID to the Helpdesk to obtain their account information to include passwords.

d. Password Change Authorization: If a user thinks the account password has been compromised, the user must change the password and notify the Cyber Security Officer. If the SA or Cyber Security Officer suspects a password has been compromised, the account must be disabled and the user and Cyber Security Manager must be notified.

e. Privileged Logins: Access to privileged logins, such as root/administrator, must be limited to the designated system administrator(s). Other users that require privileged logins must log in under their own user ID, then through the use of root equivalence protocols may be authorized access to a subset of super user command privileges (by using commands like "sudo"). This assignment of privileged access must be restricted to the minimum number of individuals necessary to effectively provide support to users or for system development, test, and production services. Users with escalated privileges (e.g. system administrators) must use separate "administrative" accounts to perform administrative functions.

f. Root Password: The root/administrator account password for each system must be recorded on paper in a memo and forwarded in a sealed envelope, or written and sent by encrypted email,

to the Cyber Security Officer. The Cyber Security Officer must place the envelope or printed email message in a locked container with restricted access. If the system root/administrator password is changed, the System Administrator must update the memo immediately.

g. Individual Accountability: Each individual is responsible for access accounts for which they have been granted. Accounts must not be shared unless authorized by the Cyber Security Manager.

h. Group IDs: Group IDs or scripts may be used to allow classification of users based on needs and privileges to be assigned. However, there must be no user IDs used by more than one person to access data, thus circumventing individual user accountability. Establishing generic "temp," "guest" or other similar accounts for use by multiple or temporary users is strictly prohibited unless authorized by the Cyber Security Manager for compelling mission requirements.

i. Account Deactivation and Deletion: User accounts will be deactivated immediately by the System Administrator upon notification of an individual's voluntary or involuntary termination of employment, transfer or retirement. Deactivated user accounts will be deleted after 90 days unless the Cyber Security Manager has approved an exception. An exception must clearly state the justification for the action and the new date for account deletion. Student accounts will remain active 30 days after the student has graduated. No additional exceptions will be granted unless the student remains at the University. In this case, the status of the student will change, to faculty or staff and the appropriate change reflected in the user account.

j. Changing Passwords: Password must be changed every 60 days at a minimum. For those users with escalated privileges (e.g. Systems Administrators), passwords must be also be changed every 60 days at a minimum. Default administrator accounts and root accounts will be changed every six months or when a SA has changed.

k. Expired Password: Users will be notified 14-days prior to password expiration that it must be changed. If the password is not changed within 14 days, the account will be locked and the user must contact the SA to reset the password.

l. Change Authorization: Users (other than the System Administrators, Cyber Security Officer) must be permitted to change only their own passwords. To ensure compliance, users are required to enter their old password as part of the changing procedure.

m. Login to a Connected System: Users must be required to authenticate their identities at login time by supplying their user ID along with their password. Privileged logins to the system, such as "root/administrator" logins, must not be directly accessed in order for system logging to be effective. Instead, system users must use their own uniquely identifiable account, and if required to perform their job function, enabling super-user equivalence using commands such as "su". It is recommended that some form of trusted identification forwarding be used between hosts when users connect to other AIS in the network. When trusted identification forwarding is not used, a remote host must require the user's ID and password when logging in through a network connection.

n. Remembering Passwords: It is recommended that users memorize their passwords and not write them on any medium. If passwords must be written, they must be protected in a manner consistent with the damage that could be caused by their compromise. A suggested method is to write the password and seal it in an envelope with the seal signed by the user selecting the password. Store the envelope in a secure location, such as a safe or locking file, to be accessed when necessary.

o. Password Validation and Audit: The Cyber Security Manager must ensure compliance with password security requirements at least every six months. Password integrity must be verified through the use of password checking routines and/or scanners. Auditing of the password files must be performed to include the date and time of the event.

p. Non-compliance: Windows user passwords will be automatically checked by active directory for compliance with the password policy at the initial password change. Non-Windows systems such as GroupWise and Linux are the responsibility of the SA and the end user to ensure that the passwords comply with this policy until an automated system can be acquired. Non-compliance with this policy could lead to disabling of the account or blocking of the system from the network until compliance it met.

4. Revision History.

CHANGE / REVISION RECORD			
Date	**Page/Paragraph**	**Description of Change**	**Made By:**
May 2014		Annual Review	jrobertson

Cyber Security Policy Guidance

1. Purpose.

This document establishes guidance and assigns the roles and responsibilities needed to ensure that sufficient security safeguards are implemented within the USU to comply with DoDI 8500.1, "Cyber Security" (*reference a.*) and the DoD Defense-in-Depth Cyber Security strategy. Adherence to the provisions in this guidance ensures that an appropriate and consistent level of security is achieved to maintain availability, integrity, authentication, confidentiality, and non-repudiation of the USU Information Systems (IS'). As per DoDI 8500.1, "Cyber Security" (*reference a.*) and Enclosure 2 (Definitions), the term "Information System" encompasses all Automated Information System Applications, Enclaves, Outsourced Information Technology (IT)-based Processes and Platform IT Interconnections. The information systems within the USU will be assigned a Mission Assurance Category as well as a Confidentiality Level and must comply with the Cyber Security controls established in DoDI 8500.1, "Cyber Security" (*reference a.*). Medical information has been designated as Sensitive Information (SI), and is to be handled in accordance with this guidance.

This guidance directly supports the mission of USU by applying the principles of DoD IT management. This includes developing and implementing policies, procedures, programs, and technical standards necessary to acquire, manage, integrate, and secure information technology systems and capabilities that support the delivery of high quality, cost effective health care services across the operational continuum. It incorporates security safeguards directed by the Federal Government and DoD, and provides information on security best practices developed as a result of several partnerships. Some of those partners include the National Institute of Standards and Technology, National Security Agency, corporate America, and other organizations committed to sharing best practices in efforts to achieve Cyber Security on a global scale.

2. Scope.

The provisions of this guidance apply to all USU IS, military personnel, DoD civilians, and contractors, who manage, design, develop, operate, or access DoD ISs, and USU developed and operated ISs, or access DoD data. Additionally, ISs include:

a. USU IS that support special environments, such as the systems used to manage and operate research equipment or projects.

b. Platform IT interconnections, e.g., sensors, medical technologies, or utility distribution systems, to external networks. Platform IT interconnections have readily identifiable security implications, essential to mission performance, and provide data exchange to enclaves. An example of a Platform IT interconnection might be a lab device that stores Protected Health Information (PHI)/(PII) and interconnects to the network.

c. Information systems under contract to USU.

d. Outsourced information-based processes such as those supporting e-Business or e-Commerce processes.

e. Stand-alone information systems.

f. Mobile computing devices such as laptops, handhelds, and personal digital assistants operating in either wired or wireless mode, or other information technologies as may be developed.

g. Biomedical technologies/devices that may or may not interconnect with a network, but process and store sensitive information.

3. Guidance.

a. USU protects the availability, integrity, authentication, confidentiality, and non- repudiation of information processed on ISs and effectively and efficiently manages the risks encountered.

b. USU shall conduct a thorough investigation and inventory of all systems to determine where DoD data is accessed, stored, received, processed, or transmitted in order to provide the requisite protection as required by this guidance. Areas of concern include but are not limited to: sites where transcription coding services take place (individual homes), bio-medical and wireless devices, networks, workstations, and special servers outside of the network.

c. Security Life Cycle Management - Security Life Cycle Management incorporates operational requirements for security in all IS planning and design, as well as ensures conformance with applicable security regulations, policies, and requirements. This information, as well as a Configuration Management Plan, comprise the Security Life Cycle Management Plan in accordance with DoDI 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)" *(reference u)*. A Security Life Cycle Management Plan shall include the following system description elements:

1) Mission of the system.

2) Functions the system will perform.

3) Interfaces with other systems.

4) Interactions across system interfaces.

5) Expected users of the system.

6) Information categories to be processed.

4. Cyber Security requirements for ISs shall be defined in detail in the Security Life Cycle Management Plan, and all minimum mandatory Cyber Security requirements established by the USU Cyber Security Manager shall be met.

5. Governance - The USU Cyber Security Branch governance consists of those functions that contribute to the effective implementation of the Cyber Security program. They are program management, planning, budgeting, staffing, and performance measurement.

6. Program Management – The USU Cyber Security Branch thru the Director, Network Operations and Communications (NOC), shall create, program, budget, operate, maintain, and measure the performance of a Cyber Security Program that provides strategic and tactical Cyber Security direction, plans, and objectives.

7. Program Planning – During the creation of the Program Objective Memorandum (POM), Cyber Security requirements shall be included for each support system, application, and IT system to ensure adequate resources are available for IT programs during their entire life cycle.

8. Program Budgeting – NOC shall budget and account for Cyber Security requirements and expenditures in the support of managing risk to their IT assets.

9. Program Staffing – Staffing of the USU Cyber Security Branch shall be limited to highly qualified Cyber Security professionals. The skill mix of the team must insure competency in planning, programming, budgeting, budget execution, and performance measurement. The Cyber Security staff may function as project and contract managers for Cyber Security support and services developed or acquired by the USU.

10. Program Performance Measurement – Processes shall be established, implemented, and managed by the USU Cyber Security Branch that will provide executive leadership with a view of how well the Cyber Security program is working throughout the USU.

11. Certification and Accreditation (C&A)

a. All ISs governed by this guidance are subject to a comprehensive Certification and Accreditation process in accordance with DoDI 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)."

b. All DoD ISs shall be reaccredited at least every three years or more frequently if deemed necessary due to IS modification or changes in the operating environment.

12. Risk Management – Assessing risk ensures that new threats and vulnerabilities are identified and appropriate security countermeasures are implemented. Risk assessments shall be conducted whenever significant and major changes occur or when new threats are identified to the DoD IS or the IS operating environment.

13. Risk Analysis – When a change is made that may impact security posture, USU shall conduct an independent full risk analysis and assessment of each of their ISs to identify potential new vulnerabilities and to verify current security safeguards continue to provide adequate protection.

14. Penetration Testing – USU shall attempt to exploit network security vulnerabilities using penetration testing during the C&A process, or more frequently as required by the USU Cyber

Security Branch. Penetration tests on DoD ISs will be conducted by the Computer Network Defense Service Provider (CNDSP), DISA Global Network Support Center (GNSC), in coordination with the Cyber Security Branch, to verify the adequacy of security counter measures in place.

15. Vulnerability Assessments – USU shall identify system and network vulnerabilities through use of vulnerability assessment tools. Vulnerability assessments shall be conducted on the network and critical servers and systems at least annually.

16. Contingency Plans – USU shall incorporate contingency plans as a part of their IS security program to ensure the availability of critical resources and facilitate the continuity of operations during an emergency or during an unexpected event. For additional Contingency Planning guidance, refer to National Institute of Standards and Technology, Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems" (*reference a.*), and the FIPS Pub 87, "Guidelines for ADP/IT Contingency Planning" (*reference b*).

a. Cyber Security Officers (ISSOs) and System Administrators (SAs) shall coordinate the development of contingency plans that address Continuity of Operations Plans and Disaster Recovery Plans.

b. Management at all echelons, including Cyber Security Managers, Cyber Security Officers and SAs must actively participate in the planning and testing of contingency plans at least annually.

c. Plans must be tested under realistic operational conditions; the results of such tests shall be documented.

17. Configuration Management – USU shall develop, implement, and maintain a configuration management plan that is defined in the System Security Authorization Agreement (SSAA) or like document. Detailed guidance exists in National Computer Security Center – Technical Guidance (TG)-006, "A Guide to Understanding Configuration Management in Trusted Systems" (*reference x.*) and in Military Handbook (MIL-HDBK) - 61A, "Configuration Management Guidance" (*reference c.*).

a. No changes to the configuration of an IS shall be made until the Cyber Security evaluates the effect(s) the proposed change will have on the security countermeasures in place on the IS. Those changes will be forwarded to the Change Control Board (CCB) for approval or recommended approval to the Designated Approving Authority (DAA) for major changes that significantly change the IS. The approval must be formally documented and reflected in the USU Service Center CMDB. .

b. During the life cycle of the IS, a configuration management plan shall be in place for security-relevant hardware, firmware, and software.

c. Cyber Security Officer and SAs maintain control of changes to the formal model as documented in the CMDB.

d. Tools shall be available and maintained under strict configuration control for comparing a newly generated version of software with the previous version. These tools must ascertain that only the intended changes have been made in the code that will be used as the new version of the IS.

e. Documentation of hardware and software configurations and diagrams shall be established and maintained to allow resumption of operations after a hardware/software failure.

18. Contract Management – USU guidance requires that Cyber Security requirements be properly reflected in all USU contracts awarded for the provision of IT products and services.

a. All USU contracts for the provision of Cyber Security and Cyber Security-enabled products or services shall include a restriction to use only properly evaluated and validated products, as required by DoDI 8500.1 "Cyber Security," *(reference a.)*.

b. All USU contracts for the provision of Cyber Security and Cyber Security-enabled products or services shall include requirements for protection of DoD SI and shall be monitored for compliance.

c. USU contracts for Cyber Security services shall include a statement that selected labor categories in RFPs or SOWs may be designated Information Technology (IT) sensitive positions or national security positions. Contractor personnel who will need access to unclassified information systems may be assigned to one of three position sensitivity designations: ADP-I (Privileged), ADP-II (Limited Privileged) and ADP-III (Non-Privileged). Contractor personnel requiring access to sensitive or classified information must have or be capable of obtaining a favorable adjudication of an investigation into their background.

19. Incident Reporting and Response.

a. USU shall have a comprehensive process to audit, detect, isolate, and react to intrusions, service disruptions, and incidents that threaten the security of operations.

b. USU shall report incidents in accordance with pre-established escalation procedures for the affected IS. GNSC and USCYBERCOM provide assistance in identifying, assessing, containing, and countering incidents that threaten DoD ISs.

c. All users shall immediately report all suspected or confirmed virus, worm, and malicious logic instances to the Cyber Security Officer thru the Customer Support Help Desk.

20. Security Awareness, Training, and Education.

a. All USU personnel shall be informed of applicable organizational policies and procedures concerning DoD ISs and shall be expected to act effectively to ensure the security of system resources. Initial and annual user security training and awareness will ensure all users are aware of security issues and what actions to take when an event or incident occurs.

b. A Cyber Security training and awareness program shall be maintained for all USU personnel.

c. All users shall be required to undergo security training upon initial assignment. Thereafter, individuals must receive annual refresher training to assure they continue to understand and abide by USU policies and procedures governing Cyber Security.

d. Training shall be tailored to information the user needs to know to operate the IS securely.

e. Personnel with security-specific responsibilities will require additional specialized training.

21. Physical Security.

a. The DoDI 5200.8-R, "Physical Security Program" (*reference d.*) and FIPS Pub 31, "Guidelines for Automatic Data Processing Physical Security and Risk Management" (*reference e.*) provide guidelines to be used by federal organizations in structuring physical security programs.

b. Facility management shall develop physical security plans that incorporate IS physical security. These policies shall be based on FIPS Pub 31, "Guidelines for Automatic Data Processing Physical Security and Risk Management" (*reference e.*).

c. Physical security shall be continually enforced, annually evaluated, and updated as required.

22. Personnel Security.

a. USU shall operate and maintain a Personnel Security Program in accordance with DoD 5200.2 R, "Personnel Security Program" (*reference f.*) A level of trustworthiness shall be established before personnel are granted access to DoD ISs or DoD sensitive information. DoD requires all DoD military and civilian personnel, contractor employees, consultants, and other designated persons affiliated with the DoD who manage, design, develop, operate, or access a DoD IS or process DoD information, to undergo an appropriate background investigation and security awareness training before access is granted to an IS or DoD information.

b. Separation of Duties - Roles and responsibilities shall be separated in accordance with OMB Circular A-130, "Management of Federal Information Resources" (*reference g.*) which requires that key duties and responsibilities in authorizing, processing, recording, and reviewing official transactions are separated among individuals, and that managers exercise appropriate oversight to ensure that individuals do not exceed or abuse their assigned authorities. The USU Cyber Security Branch requires that roles and responsibilities be separated to avoid any conflict of interest.

23. Employee Behavior.

a. DoDD 5500.7-R, "Joint Ethics Regulation" (*reference h.*) establishes federal ethics for use of Government resources to include use of the internet. The USU may provide civilian

employees and assigned military personnel, temporary workers, independent contractors, and agents access to the internet to perform assigned business functions. Individuals shall be notified of their privacy rights and security responsibilities when attempting access to DoD ISs.

b. Internet/E-mail Ethics:

1) Internet/e-mail systems and commercial systems paid for by the Federal Government shall be for official use and authorized purposes only except as noted in DoD 5500.7-R, "Joint Ethics Regulation" (*reference h.*).

2) Official use includes emergency communications and communications that are necessary in the interest of the Federal Government.

3) Incidents of unauthorized activity or misuse or abuse of the internet or e-mail use will be investigated and the perpetrator shall be subject to disciplinary action and/or monitoring action as appropriate.

4) USU personnel shall not transmit SI or PHI/PII via the internet/e-mail or other electronic means unless appropriate security controls (e.g., encryption, Public Key Infrastructure (PKI)) are in place.

24. Identification and Authentication

a. User identification and password systems support the minimum requirements of accountability, access control, least privilege, and data integrity. DoD IS users shall be granted access only to the resources they need to perform their official functions. The features and practices described in Computer Security Center Standard CSC-STD-002- 85, "Department of Defense Password Management Guideline," (*reference i.*) shall be incorporated into DoD IS'.

b. Password Management – DoD IS access is gained through the presentation of an individual identifier and password. For DoD IS' utilizing a logon ID as the individual identifier, the Cyber Security Officer, SA, and user shall ensure passwords, at a minimum, meet the requirements identified in CSC-STD-002-85, "Department of Defense Password Management Guideline" (*reference i.*) and the USU Password Policy.

c. Public Key Infrastructure – The use of PKI is a method to achieve non-repudiation by which the sender of information is provided with proof of delivery and the recipient is assured of the sender's identity so that neither can later deny having processed the information. The use of PKI certificates for authentication of a user's or systems identity shall be in accordance with published DoD policy and procedures (*references n.-s.*). These technologies shall be incorporated in systems containing SI or PHI/PII. Where interoperable PKI is required for the exchange of unclassified information with vendors and contractors, the USUHS shall only accept PKI certificates obtained from a DoD-approved external certificate authority or other mechanisms approved in accordance with DoD policy.

25. Audit Logs and Review.

a. Audit Logging – The system must record all transactions, updates, changes, and accesses to DoD ISs in audit logs. The system must create and maintain an audit trail so actions affecting the system can be traced back to the responsible party based on individual identity. The system must also protect the audit information from modification or unauthorized access or destruction.

b. Audit Review - Audit records for DoD ISs shall be reviewed by the USU Branch during the C&A process. Individual SAs shall utilize an automated tool to review audit records for DoD ISs daily or manually on a weekly basis or more frequently when deemed necessary. In those cases where an intrusion or other unauthorized act may have taken place, the audit logs shall be secured and reviewed, as soon as possible, by the appropriate authorities. Optimum use shall be made of data reduction or other automated audit log management tools.

26. Data Integrity.

a. Safeguards shall be implemented to detect and minimize inadvertent modification or destruction of data, and to detect and prevent malicious destruction or modification of data.

b. Virus protection shall be installed, enabled, and maintained on all DoD ISs.

c. Security monitoring shall occur within USU. The IS owners shall ensure the ISs under their purview are regularly monitored, system records are reviewed on a weekly basis, and that all DoD ISs are protected by Intrusion Detection Systems (IDS).

27. Production, Input, and Output Controls.

a. Production controls used for the marking, handling, processing, storage, and disposal of input and output information and media, as well as labeling and distribution procedures shall be placed on USU information and media to include printers, fax machines, copiers and biomedical devices (DoDM 5200.1, "Information Security Program" (*reference p.*)). Production controls shall be identified during the requirements phase of the system life cycle management or acquisition process.

b. Sensitive information (SI) is information, whose loss, misuse, or unauthorized access to or modification could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled. All output shall be marked to accurately reflect the sensitivity of the information. The marking may be automated (e.g., the IS has a feature that produces the markings) or may be done manually. When SI information is included in DoD documents, it shall be marked as if the information were For Official Use Only as defined in Title 17, United States Code, Section 106, "Copyrights" (*reference t.*).

c. Electronic Storage Media/Equipment Disposition - Sanitization, documentation, labeling and disposition of all unclassified electronic storage media/equipment shall be accomplished consistent with DoD requirements. Proper sanitization of electronic storage media/equipment that has been used for patient sensitive information is vitally important to USU and must follow DoD guidelines as outlined below. In addition, sanitization documentation must be maintained for a minimum of six years to ensure compliance with HIPAA security requirements.

d. Electronic storage media/equipment under vendor warranty or maintenance contract do not have to be sanitized prior to transfer from Government control to the vendor/contractor. Maintenance contracts should be written to affirm the protection of the DoD information and especially patient sensitive information by the contractor/vendor. If the electronic storage media/equipment is to be disposed of outside of Government control, the information owner must use the approved methods and procedures found in Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Memorandum, "Disposition of Unclassified DoD Computer Hard Drives," June 4, 2001 *(reference aa.)* and accompanying attachments. Although the memorandum deals primarily with DoD computer hard drives, USU guidance dictates disposition of all electronic storage media in accordance with the above memorandum. See USU Sanitization Policy.

e. The term "electronic technology storage media/equipment" as used herein means any permanent or semi-permanent electronic storage technology including, but not limited to: hard drive storage devices used in computers or biomedical equipment, back-up tapes, and removable magnetic or optical media and electronic computer equipment.

28. Software Usage.

a. Regardless of the mission assurance category or confidentiality level of the USU information system, all incorporated Cyber Security products and Cyber Security-enabled products that require use of the product's Cyber Security capabilities, acquired under contracts executed after July 1, 2002, shall comply with the evaluation and validation requirements of NSTISSP No. 11 (*reference bb.*). Qualifications and other considerations may be found in paragraph E.3.2.5, DoDI 8500.1, "Cyber Security" (*reference a.*).

b. USU activities with a mission-related requirement for installing other than government purchased software must obtain approval from the CCB.

c. Users shall abide by Section 106 of Title 17, United States (U.S.) Code, "Copyrights" (*reference t.*), which gives copyright owners exclusive rights to reproduce and distribute their material.

d. Copyrighted software products are not to be reproduced except to the limit provided by contract (e.g., archive copy for backup).

29. Wireless IT.

a. When incorporating wireless services, devices, and technological implementations within the USU Components, it shall be in accordance with DoDI 8500.1, "Cyber Security (*reference a.*). In that wireless technology (e.g., infrared, acoustic, radio frequency) can store, process, and/or transmit information outside the physical confines of the USU and introduces additional vulnerabilities, they shall not be connected to USU systems without the approval of the appropriate DAA.

b. Classified information shall not be stored, processed, and/or transmitted on USU wireless devices.

c. Only wireless devices that are procured, configured, maintained, and owned by the Government shall interface with DoD ISs.

d. Wireless devices shall incorporate the provisions of NIST and DISA guidelines for incorporating security settings.

30. Guidance Change Development.

a. Responsibility for implementing changes to this guidance rests with the USU Cyber Security Manager or the USU Chief Information Officer (CIO).

b. When new DoD or applicable national level guidance, such as Federal regulations or public laws, are promulgated or changes to existing Cyber Security policies occur, the USU Cyber Security Manager shall assess their impact on this guidance. The Cyber Security Manager will propose and present changes to modify, include, or exclude specific sections of this guidance.

c. It is the responsibility of the USU CCB members to review new policies or updates to policies and assess their impact on this guidance. The NOC Branch Chiefs will propose and present changes to modify, include, or exclude specific sections of this guidance. These suggestions will be assessed by the USU Cyber Security Branch and presented to the CCB voting members for information, comment, and proposed alternative resolutions within 60 days of submission.

d. Guidance Change Process:

1) When new guidance or a change to existing policy is required, the Cyber Security Manager will develop a draft of the proposed change.

2) The USU CCB members will be presented with proposed Cyber Security guidance or policy changes for review, comment, and concurrence.

3) After CCB coordination and concurrence, the draft guidance will be provided to the AISAC for review and comment.

4) The draft guidance will then be briefed to the USU CIO to request approval for presentation of the draft guidance to the DAA.

5) Once the AISAC has presented the draft guidance to the CIO and has received approval, the accepted guidance is forwarded through the USU CIO to the DAA for signature.

6) The signed guidance will be promulgated for implementation and documentation maintained by the CCB.

31. Roles and Responsibilities.

a. One of the most important elements of the USU Cyber Security Program is ensuring that personnel are aware of their roles and responsibilities in maintaining the security of DoD ISs, as well as all sensitive information. Personnel who manage, design, develop, program, operate, or use DoD ISs have responsibilities that contribute toward the success of the USU Cyber Security Program. Cyber Security functions may be performed full time by an employee in an IT position, or part time by an employee in a designated Cyber Security role as a collateral or adjunct duty. The position titles utilized in this guidance reflect USU nomenclature, but it is acceptable for USU contractors to have personnel with equivalent responsibilities and position titles fulfilling these requirements.

b. The USU Chief Information Officer (CIO) shall:

1) Fulfill the role of the USU senior official responsible for the development, implementation, maintenance, and oversight of the USU Cyber Security program. In this capacity, the CIO shall provide strategic and tactical program direction, allocate necessary program resources, and exercise authority over all programmatic components as necessary to accomplish USU Cyber Security goals and objectives.

2) Ensure that Cyber Security is integrated into all policies and procedures used to plan, procure, develop, implement, and manage the USU infrastructure and ISs.

3) Ensure that Cyber Security is integrated into the USU enterprise architecture.

4) Formally appoint a Cyber Security Manager in accordance with DoDI 8500.1, "Cyber Security".

5) Define strategic Cyber Security goals, annual objectives, and ensure that such goals and objectives are funded and tracked.

6) Delegate responsibilities for program implementation to Component Heads as appropriate.

c. The USU Cyber Security Manager shall:

1) Establish, manage, and assess the effectiveness of the USU Cyber Security Program.

2) Develop and promulgate Cyber Security guidance.

3) Ensure Risk and Vulnerability Assessments are accomplished for all DoD ISs with Service-specific ISs being the responsibility of the Service CIOs.

4) Provide C&A services.

5) Provide Cyber Security architecture support.

6) Ensure security awareness, education, and training is conducted.

7) Manage the Cyber Security Vulnerability Management (CSVM) program.

8) Be formally appointed in writing.

d. Designated Approving Authority (DAA)

1) USU DAAs are formally appointed and assigned in writing by the Assistant Secretary of Defense (Health Affairs) (ASD(HA)). A DAA shall be formally appointed in writing for each DoD IS operating within or on behalf of USU, to include outsourced business processes supported by private sector ISs and outsourced information technologies. The DAA shall be a U.S. citizen, a DoD employee, and possess the level of authority required to formally accept the risk for operating DoD ISs under his/her purview.

1) DAAs shall:

a) Review and formally approve DoD IS security safeguards, and issue accreditation statements that are based upon the acceptability of the security safeguards and associated level residual risk for each IS under his/her purview.

b) Grant an Approval To Operate (ATO) for DoD IS meeting USU Cyber Security requirements.

c) Grant an Interim Approval to Operate (IATO) for DoD ISs meeting DIACAP requirements for an IATO. The IATO shall not exceed a 12-month period during which all security issues required to meet an ATO accreditation shall be satisfactorily resolved.

d) Ensure ISs under development are accredited prior to deployment. Identify security deficiencies and, where the deficiencies are sufficiently serious to preclude accreditation, take appropriate action to achieve an acceptable security level.

e) Establish and verify for each IS under his/her purview data ownership, accountability, access rights, and special handling requirements.

f) Verify that an appropriate mission assurance category has been assigned for each IS under his/her purview.

g) Ensure that Cyber Security Managers, Cyber Security Officers, and SAs are formally designated and assigned in writing for all ISs under his/her purview, and that they receive the level of training and appropriate certifications necessary to perform the tasks associated with assigned responsibilities.

h) Ensure a process for managing information security incidents that includes prevention, detection, response, and lessons learned is developed, implemented and maintained for all ISs under his/her purview.

i) Ensure continuous life-cycle oversight and surveillance of the security safeguards approved during the C&A process through establishment of surveillance plans, performance metrics and reporting procedures to monitor Cyber Security compliance with guidance.

j) Ensure a security education, awareness, and training program that addresses all USU personnel categories, to include general users, IT professionals, managers, and senior executives is developed, implemented, and maintained for all ISs under his/her purview.

k) Ensure that documented Memorandums of Agreement (MOAs) to address security requirements are in place for all ISs under his/her purview that interface or are networked, and managed by different DAAs.

l) Ensure that documented MOAs to address security requirements are in place for all ISs under his/her purview that interface or are networked to non-DoD entities.

m) Ensure the reaccreditation of ISs under his/her purview at least every three years, or more frequently if deemed necessary due to major IS modifications or like modifications to the operating environment.

n) Formally appoint and assign in writing Designated Approving Authority Representatives (DAARs) and Certifiers for select ISs under his/her purview, as deemed appropriate. The DAAR has the same responsibilities as the DAA, can approve an initial IATO, and will ensure that any and all subsequent IATO requests are forwarded to the appropriate DAA for review and approval.

e. Certifier

1) The Certifier for USU IS is designated by the USU DAA with the authority to establish and manage the University's C&A process and to verify and validate IS security design and implementation through testing and review of IS security documentation.

2) The Certifier shall:

a) Ensure a comprehensive, standardized risk analysis and security evaluation is completed prior to IS certification.

b) Certify the extent to which ISs meet prescribed security requirements.

c) Prepare the IS C&A report and forward the complete report with recommendations on accreditation to the appropriate DAA.

d) Maintain and provide other records and reports of C&A activities, as necessary.

f. Cyber Security Officers

1) The Cyber Security Officers ensures that the systems under his/her purview are operated and maintained at the appropriate level of security, oversees the implementation of all applicable IS security requirements, and monitors IS security operations. In addition to the roles and responsibilities identified in DoDI 8500.1, "Cyber Security" (reference a.), Cyber Security Officers shall:

a) Act in the capacity of Cyber Security expert for ISs under his/her purview, and as such shall be responsible for coordinating Cyber Security issues with the USU Cyber Security Branch. The Cyber Security Officer also serves as a Cyber Security advisor to the Certifier, the Cyber Security Manager, and the DAA.

b) Ensure that ISs are operated, used, maintained, and disposed of in accordance with all applicable Cyber Security policies and procedures.

c) Enforce Cyber Security policies and safeguards for all personnel afforded access to the IS for which the Cyber Security Officer has cognizance.

d) Comply with DoD 5200.2-R, "Personnel Security Program" (*reference f.*) governing personnel security clearances and the designation of automated data processing (ADP)/IT positions and security investigation requirements.

e) Ensure that users have the required authorization and need-to-know, have been indoctrinated, and are familiar with internal security practices before being granted access to the IS.

f) Prepare a C&A Plan for ISs under his/her purview.

g) Ensure IS security safeguards required for all ISs under his/her purview are addressed in the IS documentation.

h) Review audit trails for all ISs under his/her purview at least weekly or more frequently if deemed necessary.

i) Report incidents to the DAA and the DoD reporting chain, as required, and coordinate responses to Cyber Security-related alerts.

j) Develop and provide reports on the Cyber Security posture of all ISs under his/her purview as required by the DAA.

k) Ensure that security procedures and protocols governing IS operations are developed, promulgated, and maintained for ISs.

l) Ensure consistent progress toward site accreditation of all ISs under his/her purview.

m) Ensure adherence to CSVM procedures and processes.

n) Ensure the development, maintenance, and annual testing of required contingency plans.

o) Ensure individual access to a particular DoD IS is revoked immediately upon determination that such access is no longer required (e.g., completion of project, transfer, retirement, resignation).

p) Complete job-specific Cyber Security training on an annual basis.

g. Privileged Users (e.g., System Administrators, Network Security Officer).

1) Privileged Users meet all USU requirements for authorized users. Privileged Users shall:

a) Ensure servers, workstations, peripherals, communication devices, application software and all other applicable IT assets are available to support users.

b) Ensure approved anti-virus software is installed, maintained, and updated on all servers and workstations under his/her purview.

c) Assist the Cyber Security Officer in maintaining IS configuration controls and access levels consistent with the need-to-know doctrine.

d) Advise the Cyber Security Officer of security anomalies or integrity deficiencies immediately upon detection.

e) Administer user identification or authentication mechanisms of all ISs under his/her purview.

f) Perform system backups, software upgrades, and system recovery, including the secure storage and distribution of backups and upgrades.

g) Coordinate with the Cyber Security Officer, as required, to enforce password controls, set permissions, perform security management functions, and coordinate and/or perform IS preventative and corrective maintenance problems. Document and report any identified vulnerabilities to the Cyber Security Officer immediately upon detection.

h) Report to the Cyber Security Officer all IS failures that could lead to unauthorized disclosure or any attempt to gain unauthorized access to DoD ISs and/or data processed, stored and/or transmitted by the IS.

i) Configure and monitor the IDS.

j) Coordinate Help Desk support as required.

k) Complete job-specific Cyber Security training on an annual basis.

2) Authorized Users shall:

a) Observe all applicable Cyber Security policies, regulations, procedures and practices governing the secure operation (e.g., protection of passwords) and authorized use of ISs.

b) Report all security incidents, potential threats, and suspected vulnerabilities to the appropriate Cyber Security Officer or Cyber Security Manager immediately upon detection.

c) Complete initial and annual security awareness training.

d) Possess the appropriate credentials (e.g., Background Investigations, Security Clearances) required for general and/or privileged levels of access to DoD ISs.

e) Access only that data, software, hardware, and firmware for which they are authorized access and have a need-to-know, and assume only authorized roles and privileges.

f) Protect all IS access authenticators, such as individual IDs and passwords, commensurate with the classification or sensitivity of the information accessed. Immediately report any compromise or suspect compromise of an authenticator to the appropriate Cyber Security Officer immediately upon detection.

g) Ensure that IS media and output are properly marked, controlled, stored, transported, and destroyed in accordance with the classification or sensitivity and need-to-know.

h) Protect terminals or workstations from unauthorized access.

i) Immediately inform the Cyber Security Officer when access to a particular DoD IS is no longer required (e.g., completion of project, transfer, retirement, resignation).

j) Observe policies and procedures governing the secure operation and authorized use of any DoD IS to which they have been granted access.

k) Use the DoD IS only for authorized purposes.

l) Not unilaterally bypass, strain, or test Cyber Security mechanisms. If Cyber Security mechanisms must be bypassed, users shall coordinate the procedure with the Cyber Security Officer and receive written approval from the Cyber Security Manager.

m) Not introduce or use unauthorized software, firmware, or hardware on the DoD IS. Users shall not relocate or in any way change, or cause to change, DoD IS equipment or the network connectivity of equipment without the proper Cyber Security Manager authorization.

Enclosures:
1. References
2. Definitions

REFERENCES

a. DoDI 8500.1, "Cyber Security," March 14, 2014

b. National Institute of Standards and Technology, Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems," June 2002

c. Military Handbook (MIL-HDBK) 61A, "Configuration Management Guidance," February 7, 2001

d. DoD 5200.8-R, "Physical Security Program," May 1991

e. Federal Information Processing Standards Publication (FIPS Pub) 31, "Guidelines for Automatic Data Processing Physical Security and Risk Management," June 1974

f. DoD 5200.2-R, "Personnel Security Program," January 1987

g. OMB Circular No. A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Systems," November 30, 2000

h. DoD 5500.7-R, "Joint Ethics Regulation," Change 4, August 6, 1998

i. Computer Security Center Standard, CSC-STD-002-85, "Department of Defense Password Management Guideline," April 12, 1985

j. DoD Chief Information Officer Memorandum, subject: "Public Key Enabling (PKE) of Applications, Web Servers, and Networks for the Department of Defense (DoD)," 17 May 2001

k. DoD PKI Program Management Office Memorandum, subject: "X.509 Certificate Policy for the United States Department of Defense," May 31, 2002

l. DoD Chief Information Officer Memorandum, subject: "Common Access Card," 16 January 2001

m. Deputy Secretary of Defense Memorandum, subject: "Smart Card Adoption and Implementation," 10 November 1999

n. Assistant Secretary of Defense Memorandum, subject: "Public Key Infrastructure (PKI) Policy Update," 21 May 2002

o. Office of the Secretary of Defense Memorandum, subject: "Common Access Card – Changes," 18 April 2002

p. DoDM 5200.1, "Information Security Program," February 24, 2012

q. Privacy Act of 1974 (Public Law 93-579)

r. Deputy Secretary of Defense Memorandum, subject: "Disposition of Unclassified DoD Computer Hard Drives," June 4, 2001

s. Freedom of Information Act of 1986 (Public Law 99-570)

t. Title 17, United States Code, Section 106, "Copyrights"

u. DoDI 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014

v. DoDD 5000.1, "The Defense Acquisition System," May 12, 2003

w. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4009, National Information Systems Security (INFOSEC) Glossary, September 2000

x. National Computer Security Center – Technical Guidance (TG)-006, "A Guide to Understanding Configuration Management in Trusted Systems," October 16, 2002

y. Deputy Secretary of Defense Memorandum, subject: "Defense Acquisition," October 30, 2002

z. Federal Information Processing Standards Publication (FIPS Pub) 87, "Guidelines for ADP/IT Contingency Planning," March 1981

aa. Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Memorandum, "Disposition of Unclassified DoD Computer Hard Drives," June 4, 2001

bb. NSTISSP No. 11, " Revised Fact Sheet National Information Assurance Acquisition Policy," July 2003

DEFINITIONS

Access – A specific type of interaction between a subject and an object resulting in the flow of information from one to the other.

Accountability – The property that enables activities on a system to be traced to individuals who may then be held responsible for their actions.

Accreditation – A formal declaration by the DAA that the IS is to operate in a particular security mode using a prescribed set of safeguards. Accreditation is the official management authorization for operation of ISs on the certification process as well as other management considerations. The accreditation statement affixes security responsibility with the DAA and shows that due care has been taken for security.

Assurance – A measure of confidence that the security features and architecture of an IS accurately mediate and enforce the security policy.

Audit Trail – A chronological record of system activities sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results.

Authenticators - Security measures such as individual account identification and passwords that are designed to verify an individual's authorization to access a system or receive specific categories of information.

Authorization – The granting of access rights to a user, program, or process by a responsible administrator.

Backup – A copy of data and/or applications contained in the IS stored on magnetic media outside of the IS to be used in the event IS data is lost.

Certification – The comprehensive evaluation of the technical and non-technical security features of an IS and other safeguards, made in support of the accreditation process, that establishes the extent to which a particular design and implementation meet a specified set of security requirements.

Compromise – A violation of the security policy of a system such that unauthorized disclosure of SI may have occurred.

Confidentiality– Assurance that information is not disclosed to unauthorized persons, processes, or devices.

Configuration Control –(1) A systematic process that ensures that changes to released configuration documentation are properly identified, documented, evaluated for impact, approved by an appropriate level of authority, incorporated, and verified. (2) The configuration

management activity concerning: the systematic proposal, justification, evaluation, coordination, and disposition of proposed changes; and the implementation of all approved and released changes into (a) the applicable configurations of a product, (b) associated product information, and (c) supporting and interfacing products and their associated product information.

Configuration Management – A management process for establishing and maintaining consistency of a product's performance, functional, and physical attributes with its requirements, design and operational information throughout its life.

Contingency Plan – A plan for emergency response, backup operations, and post-disaster recovery maintained by an activity as a part of its security program that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation.

Continuity of Operations Plan – A plan for developing advanced arrangements to stand up critical operations following an unplanned event that disrupts critical operational processes.

Countermeasure – Any action, device, procedure, technique, or other measure that reduces the vulnerability of or threat to a system.

Data – A representation of facts, concepts, information or instructions suitable for communication, interpretation, or processing by users or by an IS.

Defense-in-Depth – The security approach whereby layers of Cyber Security solutions are used to establish an adequate Cyber Security posture. Implementation of this strategy also recognizes that due to the highly interactive nature of the various systems and networks, Cyber Security solutions must be considered within the context of the shared risk environment and that any single system cannot be adequately secured unless all interconnected systems are adequately secured.

Designated Approving Authority – The official who has the authority to decide on accepting the security safeguards prescribed for an IS or that official who may be responsible for issuing an accreditation statement that records the decision to accept those safeguards.

Disaster Recovery Plan – A plan for developing advance arrangements and procedures that will enable an organization to respond to a disaster and resume its critical business operations within a predetermined period of time, minimize the amount of loss, and repair the stricken facilities as soon as possible.

Enclave - Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves always assume the highest mission assurance category and security classification of the AIS applications or outsourced IT-based processes they support, and derive their security needs from those systems. They provide standard Cyber Security capabilities, such as boundary defense, incident detection and response, and key management, and also deliver common applications, such as office automation and electronic mail. Enclaves are analogous to

general support systems as defined in OMB Circular No. A-130, "Management of Federal Information Resources" (reference g.). Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers.

Identification – The process that enables recognition of an entity by a system, generally by the use of unique machine-readable user names.

Cyber Security – Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

Cyber Security Officer – The person responsible for ensuring that security is provided for and implemented throughout the life-cycle of an AIS/network from the beginning of the concept development plan through its design, development, operation, maintenance, and secure disposal.

Cyber Security Vulnerability Alert – Comprehensive distribution process for notification of Combatant Commanders, Services, and Agencies about vulnerability alerts and countermeasures information.

Information System (IS) – A set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes AIS applications, enclaves, outsourced IT-based processes, and platform IT interconnections (NSTISSI No. 4009, "National Information Systems Security (INFOSEC) Glossary" *(reference w)*) modified to include the four DoD categories).

Integrity – Quality of an IT system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the information structures and occurrence of the stored information. It is composed of data integrity and system integrity.

Interim Approval to Operate – Temporary authorization granted by a DAA for an IS to process information based on preliminary results of a security evaluation of the system.

Need-To-Know – The necessity for access to, knowledge of, or possession of specific information required to carry out official duties.

Network – A network is composed of a communications medium and all components attached to that medium whose responsibility is the transference of information.
Non-repudiation – The method by which the sender of information is provided with proof of delivery and the recipient is assured of the sender's identity so that neither can later deny having processed the information.

Outsourced IT-based Process - For DoD Cyber Security purposes, an outsourced IT-based process is a general term used to refer to outsourced business processes supported by private

sector information systems, outsourced information technologies, or outsourced information services. An outsourced IT-based process performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed in both acquisition and operations.

Password – A protected, private character string used to authenticate an identity.

Penetration Testing – The portion of security testing in which the evaluators attempt to circumvent the security features of a system. The evaluators may be assumed to use all system design and implementation documentation, which may include listings of system source code, manuals, and circuit diagrams. The evaluator's work under the same constraints applied to ordinary users.

Personnel Security – The procedures established to ensure that all personnel who have access to sensitive information have the required authority, as well as appropriate clearances.

Physical Security – The application of physical barriers and control procedures as preventive measures or countermeasures against threats to resources and sensitive information.

Platform IT Interconnection - For DoD Cyber Security purposes, platform IT interconnection refers to network access to platform IT. Platform IT interconnection has readily identifiable security considerations and needs that must be addressed in both acquisition and operations. Platform IT refers to computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems such as weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility distribution systems such as water and electric.
Examples of platform IT interconnections that impose security considerations include: communications interfaces for data exchanges with enclaves for mission planning or execution, remote administration, and remote upgrade or reconfiguration (DoDI 8500.1, "Cyber Security " (*reference a.*).

Privileges – A set of authorization/permissions granted by an authorized officer to an AIS and network or network user to perform certain operations.

Protected Health Information (PHI) – Individually identifiable health information that is a subset of health information, including demographics, that identifies an individual or there is a reasonable basis to believe that the information may be used to identify an individual. This information is created or received by a healthcare provider, health plan, or employer and relates to past, present, or future physical or mental health of an individual; the provision of care or payment for care of that individual. PHI is information that is transmitted or maintained by electronic or any other form or medium.
Public Key Infrastructure – An enterprise-wide service that supports digital signatures and other public key-based security mechanisms for DoD functional domain programs, including generation, production, distribution, control and accounting of public key certificates.

Risk – The probability that a particular threat will exploit a particular vulnerability of the system.

Risk Analysis – The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards. Risk analysis is a part of risk management.

Risk Assessment – An assessment of a system based on the sensitivity of information processed, or to be processed, and the clearances of users to determine the security class of the system.

Risk Management – The total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost benefit analysis, selection, implementation and testing, security evaluation of safeguards, and overall security review.

Safeguards – An implementation of technology or techniques to protect confidentiality, integrity, and availability.

Security Evaluation – An evaluation done to assess the degree of trust that can be placed in systems for the secure handling of sensitive information. One type, a product evaluation, is an evaluation performed on the hardware and software features and assurances of a computer product from a perspective that excludes the application environment. The other type, a system evaluation, is done to access a system's security safeguards with respect to a specific operational mission and is a major step in the C&A process.

Security Policy – The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

Security Requirements – The types and levels of protection necessary for equipment, data, information, applications, personnel, and facilities to meet security policy.

Security Safeguards – The protective measures and controls prescribed to meet the security requirements specified for a system. Those safeguards may include but are not necessarily limited to: hardware and software security features, operating procedures, accountability procedures, access and distribution controls, management constraints, personnel security, and physical structures, areas, and devices.

Sensitive Information – Any information, the loss, misuse, modification of, or unauthorized access to, could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, U.S. Code, (The Privacy Act) but has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

System Integrity – The quality that a system has when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

Threat – Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of service.

User – Person or process accessing an IS either by direct connections (e.g., via terminals), or indirect connections (e.g., prepare input data or receive output not reviewed for content or classification by a responsible individual).

User ID – A unique symbol or character strings used by a system to identify a specific user.

Virus – A self-propagating computer program composed of a mission component, a trigger component, and a self-propagating component.

Vulnerability – A weakness in system security procedures, system design, implementation, internal controls, etc. that could be exploited to violate system security policy.

USU Demilitarized Zone (DMZ) Policy

1. Purpose.

The purpose of this policy is to establish standards for the baseline configuration of servers and devices on the DMZ that are owned and/or operated by the USU Network Operations and Communications (NOC) and external system administrators (SAs) from program offices. Effective implementation of this policy will minimize mis-configurations and unauthorized access to USU information systems (IS).

2. Scope.

This policy applies to all managed and hosted servers and devices located in the USU DMZ that are owned and operated by NOC and external system administrators.

3. Policy.

a. Ownership and Responsibilities.

Equipment and applications within the scope of this policy must be administered by the NOC or assigned SAs approved by the Change Control Board (CCB) for DMZ systems, applications, and/or network management. The NOC must be responsible for the following:

1) Equipment must be documented in the department wide enterprise management system. At a minimum, the following information is required:

a) Host contacts and location.

b) IP Address.

c) Hardware and operating system/version.

d) Main functions and applications.

e) Password groups for privileged passwords.

2) Network interfaces must have appropriate Domain Name Server records (minimum of A and PTR records).

3) Password groups must be maintained in accordance with USU Password Policy

4) Immediate access to equipment and system logs must be granted to Cyber Security team upon demand, per the audit policy.

5) Changes to existing equipment and deployment of new equipment must follow USU Change Management (CM) Plan. To verify compliance with this policy, the Cyber Security team will periodically audit DMZ equipment per the audit policy.

b. General Configuration Policy.

All equipment must comply with the following configuration policy:

1) Hardware, operating systems, services and applications must be approved as part of the pre-deployment review phase.

2) Operating system configuration must be performed in accordance with the DoD Standard Technical Implementation Guides (STIG), Cyber Security Server Policy and the Cyber Security Web Server Policy.

3) All patches/hot-fixes recommended by the equipment vendor and IAVA notices published by the Cyber Security Branch must be applied or installed. If patches cannot be applied, then the SA must submit a Plan of Action and Milestone(s) to include a mitigation strategy to the Cyber Security Officer.

4) Services and applications not serving USU requirements must be disabled.

5) Trust relationships between systems may only be introduced according to prudent security practices and must be documented. No trust relationship from a system outside the USU firewall to a system behind the firewall is permitted.

6) Services and applications not for general access must be restricted by access control lists.

7) Insecure services or protocols (as determined by Cyber Security team) must be replaced with more secure equivalents whenever such exist.

8) Port and Protocol waiver request must be submitted to the Cyber Security Branch for approval prior to deployment.

9) DMZ Whitelist Request must be submitted to the Cyber Security Branch for approval prior to deployment.

10) DNS Whitelist Requests must be submitted to the Cyber Security Branch for approval prior to deployment.

11) Remote administration must be performed over secure channels (e.g., encrypted network connections using SSH or IPSEC) or console access independent from the DMZ network. All host content updates must occur over secure channels.

12) Security-related events must be logged and audit trails saved to the log server. Security-related events include (but are not limited to) the following:

a) User login failures.

b) Failure to obtain privileged access.

c) Access policy violations.

d) See Audit Policy for additional information.

13) The CCB will review all non-compliance waiver requests on a case-by-case basis and approve waivers, if justified.

c. New Installations and Change Management Procedures.

All new installations and changes to the configuration of existing equipment and applications must follow the policies/procedures below:

1) New installations must be compliant with the DoD STIG.

2) Configuration changes must follow CM Procedures.

3) Port and Protocol waiver request must be submitted to the Cyber Security Branch for approval prior to deployment.

4) DMZ Whitelist Request must be submitted to the Cyber Security Branch for approval prior to deployment.

5) DNS Whitelist Requests must be submitted to the Cyber Security Branch for approval prior to deployment.

6) Cyber Security Officer must perform system/application audits prior to the deployment of new services.

7) NOC must be engaged, either directly or via CM, to approve all new deployments and configuration changes.

4. Non-compliance.

DMZ Servers and devices that do not comply with this policy maybe disconnected from the DMZ subnet until compliance is met.

5. Revision History.

CHANGE / REVISION RECORD			
Date	**Page/Paragraph**	**Description of Change**	**Made By:**
May 2014		Annual Review	jrobertson

Server Security Policy

1. Purpose.

The purpose of this policy is to establish standards for the baseline configuration of internal server equipment that is owned and/or operated by USU. Effective implementation of this policy will minimize unauthorized access to USU proprietary information and technology.

2. Scope.

This policy applies to server equipment owned and/or operated by USU, and to servers registered under any USU-owned internal network domain.

3. Policy.

a. Ownership and Responsibilities. All internal servers deployed at USU must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by Cyber Security. Operational groups must monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by Cyber Security.

1) Servers must be registered within the USU CMDB Network Device Matrix. At a minimum, the following information is required to positively identify the point of contact:

a) Server contact(s) and location, and a backup contact.

b) Hardware and Operating System/Version.

c) Main functions and applications, if applicable.

2) Information in the USU CMDB system must be kept up-to-date.

3) Configuration changes for production servers must follow the USU Configuration Management Plan.

b. General Configuration Guidelines.

1) Operating System configuration must be in accordance with DISA Standard Technical Implementation Guides (STIGs) guidelines.

2) Services and applications that will not be used must be disabled where practical.

3) Access to services must be logged and/or protected through access-control methods such as Group Policy Objects (GPOs).

4) The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirement

5) Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.

6) Always use standard security principles of least required access to perform a function.

7) Do not use root or the local administrative account when a non-privileged account will do.

8) If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).

9) Servers must be physically located in an access-controlled environment.

10) Servers are specifically prohibited from operating from uncontrolled cubicle areas.

c. Monitoring

1) All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

a) All security related logs will be kept online for a minimum of one week.

b) Daily incremental tape backups will be retained for at least one month.

c) Weekly full tape backups of logs will be retained for at least one month.

d) Monthly full backups will be retained for a minimum of two years.

2) Security-related events will be reported to Cyber Security, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

a) Port-scan attacks.

b) Evidence of unauthorized access to privileged accounts.

c) Anomalous occurrences that are not related to specific applications on the host.

d. Compliance.

1) Audits will be performed monthly by the Cyber Security Branch utilizing the Nessus Scanning Tool.

2) Audits will be managed by the Cyber Security Branch, in accordance with the Audit Policy. Cyber Security will filter findings not related to a specific operational group and then present the findings to the appropriate system administers for remediation, mitigation or Plan of Action and Milestone (POA&M).

3) Every effort will be made to prevent audits from causing operational failures or disruptions.

e. Enforcement

Systems that do not comply with this policy may be disconnected from the network until compliance is met.

4. Definitions.

a. DMZ - De-militarized Zone - A network segment external to the corporate production network.

b. Server -A Server is defined as an internal USU Server. Desktop machines and Lab equipment are not relevant to the scope of this policy.

5. Revision History.

CHANGE / REVISION RECORD			
Date	**Page/Paragraph**	**Description of Change**	**Made By:**
May 2014		Annual Review	jrobertson

Acquisition Assessment Policy

1. Purpose.

This policy's purpose is to establish Cyber Security responsibilities regarding USU acquisitions, and define the minimum security requirements of a Cyber Security acquisition assessment.

2. Scope.

This policy applies to all USU systems, networks, laboratories, test equipment, hardware, software and firmware, owned and/or operated by USU.

3. Policy.

Acquisition assessments are conducted to ensure that a systems being acquired by USU does not pose a security risk to the USU network, internal systems, and/or sensitive information. Cyber Security will provide personnel to serve as active members of the acquisition team throughout the acquisition process. The Cyber Security role is to detect and evaluate information security risk, develop a remediation plan with the affected parties for the identified risk, and work with the acquisitions team to implement solutions for any identified security risks, prior to allowing connectivity to USU networks. Below are the minimum requirements that the acquired system must meet before being connected to the USU network.

4. Requirements.

a. Hosts.

1) All systems (servers, desktops, laptops) will be replaced or re-imaged with a USU standard image.

2) Business critical production servers that cannot be replaced or re-imaged must be audited and a waiver granted by CCB Chair.

3) All systems will require DoD approved virus protection before being connected to the network.

b. Networks

1) All network devices will be replaced or re-imaged with a USU standard image.

2) Wireless network access points will be configured to the DoD STIG and USU standard.

c. Internet

1) All internet connections will be terminated.

2) When justified by business requirements, air-gapped internet connections require Cyber Security review and CCB approval.

d. Remote Access

1) All remote access connections will be terminated.

2) Remote access to the production network will be provided by UIS upon approval of the Cyber Security Officer.

3) All requiring remote access by contracted vendors must have a MOA and/or SLA and must be documented in the service contract.

4) All remote access must be CAC only.

e. Labs

1) Lab equipment must be physically or logically separated and secured from non-lab areas.

2) Any direct network connections (including analog lines, ISDN lines, T1, etc.) to external customers, partners, etc., must be reviewed by the Cyber Security Branch and approved by the CCB.

3) All acquired labs must meet with USU Security Policies or be granted a waiver by CCB.

4) In the event the acquired computer systems being connected to the USU network fail to meet these requirements, the Cyber Security Manger must review and document the risk through the CCB and acquire DAA approval of the risk to the USU networks.

5. Enforcement.

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Definitions.

a. Business Critical Production Server - A server that is critical to the continued business operations of the acquired company.

Digital Signature Acceptance Policy

1. Purpose.

The purpose of this policy is to provide guidance on when digital signatures are considered accepted means of validating the identity of a signer in the USU and government electronic documents and correspondence, and thus a substitute for traditional "wet" signatures, within the organization. Because communication has become primarily electronic, the goal is to reduce confusion about when a digital signature is trusted.

2. Scope.

This policy applies to all USU employees, contractors, and other agents conducting USU business with government organizations utilizing a USU-provided digital key pair.

3. Policy.

a. General Policy Statement.

1) A digital signature is an acceptable substitute for a wet signature on any government document or correspondence, with the exception of those identified by the USU Vice President, Finance and Administration (VFA).

2) The VFA's office will maintain an organization-wide list of the types of documents and correspondence that are not covered by this policy.

3) Digital signatures must apply to individuals only. Digital signatures for roles, positions, or titles (e.g. the VFA) are not considered valid.

b. Responsibilities. Digital signature acceptance requires specific action on both the part of the employee signing the document or correspondence (hereafter the signer), and the employee receiving/reading the document or correspondence (hereafter the recipient).

1) Signer Responsibilities

a) Signers must obtain a signing key pair from DoD Certificate Authority. This key pair will be generated using DoD Public Key Infrastructure (PKI) and the public key will be signed by the DoD CA.

b) Signers must sign documents and correspondence using software approved by the USU CCB.

c) Signers must protect their private key and keep it secret.

d) If a signer believes that their private key was stolen or otherwise compromised, the signer must contact Cyber Security Branch immediately to have the signer's digital key pair revoked.

2) Recipient Responsibilities

a) Recipients must read documents and correspondence using software approved by CCB.

b) Recipients must verify that the signer's public key was signed by the DoD Certificate Authority (CA), by viewing the details about the signed key using the software to read the document or correspondence.

c) If the signer's digital signature does not appear valid, the recipient must not trust the source of the document or correspondence.

d) If a recipient believes that a digital signature has been abused, the recipient must report their concern to the Cyber Security Branch immediately.

4. Enforcement.

Any employee found to have violated this policy is subject to disciplinary action including, without limitation, termination.

5. Definitions.

Certificate Authority (CA). A trusted entity by all parties in a transaction that is used to verify the identities of those parties by signing the public key.

Digital Key Pair. A private key and its corresponding public key. The private key is used to create the digital signature, and the public key is used to verify that its corresponding private key created the digital signature.

Digital Signature. An electronic identifier created with a signer's private key that allows the recipient to determine whether or not the identifier was created by the signer's private key, and whether the initial signed message has been altered.

Public Key Infrastructure (PKI). PKI is the collection of systems and applications that comprise an organization's ability to issue digital key pairs.

Wet Signature. An original written identifier or mark manually placed on a physical page; a traditional signature.

6. Revision History.

CHANGE / REVISION RECORD			
Date	**Page/Paragraph**	**Description of Change**	**Made By:**
May 2014		Annual Review	jrobertson

Procurement of Desktop and Laptop Computing Systems

1. Purpose.
This Instruction establishes policies, assigns responsibilities, and provides procedures related to the acquisition of desktop and laptop systems.

2. References. *See Enclosure 1.*

3. Applicability.
This Instruction applies to the purchase of all faculty, staff, student and contractor desktop and laptop computing systems regardless of funding source.

4. Policy.
The following paragraphs provide University policy on specific topics.

a. One System Per User.

1) Billeted faculty, staff, and contractors, who are assigned to the campus, AFRRI, or its official extensions, are provided a computer system to perform daily routine office automation tasks. Due to the escalating cost of maintaining systems, information security requirements and in recognition of an increasingly mobile work force, USU will provide, from a single vendor, either one desktop or one laptop computer with docking station to personnel based on individual mission needs. Multiple systems purchased with O&M funds, simply to accommodate travel or tele-work, is not authorized.

2) Approval for the provision of a laptop for mobile workers is the responsibility of the immediate supervising Dean, Department Chair, Vice President or Assistant Vice President. The desktop versus laptop decision should be based on the person's requirement to perform work outside of the office, beyond normal working hours, through approved telecommuting plans or to meet frequent travel needs. Request must be submitted utilizing the USU Service Center in conjunction with scheduled computer replacements or upon appointment of a new position for those with a laptop requirement.

3) Allocation of laptops will occur based on the USU computer replacement program which replaces a desktop every four years and a laptop system on a three-year cycle. If funding is not sufficient to procure the number of requested laptops during a refresh period, the user may be provided a desktop and the laptop request filled in the next refresh or as additional funds become available.

4) A small number of laptops will be maintained by NOC and made available for temporary "sign-out" for personnel with only occasional mobile computing needs. Sign-outs are on a first come, first served basis. Temporary laptop requests can be made via the USU Service Center.

b. Grant Funded Systems.

1) This policy does not preclude the acquisition of additional computing systems to support grant funded research and/or systems required for scientific equipment and server operation; however, in an effort to maintain uniformity, the USU single vendor desktop and/or laptop must be considered prior to purchase of different IT equipment.

2) In cases where the single vendor desktop or laptop meets all of the grant minimum IT requirements, a single vendor system will be procured. Other systems are authorized for procurement when minimum IT requirements cannot be met.

3) Scientific IT equipment, server, and non-single vendor desktop/laptop acquisitions will be reviewed by the Automated Information Systems Advisory Committee (AISAC) before procurement. The AISAC approval form can be found in Enclosure 2. Failure to obtain prior approval may result in return or reassignment of the equipment.

4) This policy also applies to HJF procured desktops and laptops unless the system will not be placed on the USUHS .mil or .edu networks.

c. Information Security.

Desktops and laptops, regardless of source of procurement, are University information systems and whether connected to the USU network or operated outside that network, must be in compliance with Federal, DoD, and DHA security requirements. Laptops, based on their mobile nature, are subject to specific security scans to ensure compliance with regulations. Laptop users are required to log on to the USU network at least once a week to ensure that proper security and maintenance patches are applied to the system.

Enclosures:

1. References
2. Automated Information Systems Advisory Committee (AISAC) Information Technology Approval Form

REFERENCES

(a) U.S. Executive Office of the President, Office of Management and Budget (OMB) Bulletin No. A-130, "Management of Federal Information Resources." Appendix III, "Security of Federal Automated Information Resources," February 1996

(b) DoDD 5200.1, "DoD Information Security Program," December 13, 1996

(c) BUMED Field Information Security Policy Manual, Version 1.04, May 2001

(d) USU Instruction 5201, "Information Security Program," April 7, 1995

(e) USUHS Instruction 5202.2, "Electronic Information and Communication Policies," January 2, 2001

(f) Final FAR Rule for Implementing Section 508 of the Rehab Act Electronic and Information Technology Accessibility for Persons with Disabilities, April 25, 2001

(g) DoD Directive 5500.7-R "Joint Ethics Regulation," August 1993

AUTOMATED INFORMATION SYSTEMS ADVISORY COMMITTTEE (AISAC)
INFORMATION TECHNOLOGY APPROVAL FORM

NAME_____ **DATE:** _____

DEPT: ___ ___ ___ **ROOM:** _____ **PHONE:**_____

EMAIL: _____

REQUEST IS FOR: _____

Item Requested: _____

__ Non-single vendor (non-leased) Desktop __Server
__Non-single vendor (non-leased) Laptop __Tablet
__Special Software
__Other_____

Cost (Include purchase, installation and Maintenance): _____

_____

Funding Source:_____

Use:_____

_____

__ For UIS Operation __For local Operation

Network Requirements: _____

Security Systems: _____

Systems Administrator: _____

AISAC Recommendation:_____

_____

Internet and E-Mail Privacy Policy

1. Purpose.

The purpose of this policy is to establish standards to all faculty, staff, civilians, and contractors that utilize USU owned e-mail and internet connectivity to conduct USU business. Effective implementation of this policy will minimize mis-configurations and unauthorized access to USU information systems (IS).

2. Scope.

This policy applies to all faculty, staff, civilians, and contractors, who plan, deploy, configure, operate, or maintain data communications resources, Cyber Security systems, or firewall devices directly or indirectly attached to USU networks. Internet and e-mail systems are USU systems used for conducting general operational and administrative tasks and provide a vehicle for communicating electronically with internal and external agencies. It provides a reliable and timely method of exchanging information and eliciting responses among staff, students, and partners.

3. Responsibilities.

a. Managers must make all personnel aware of the rules associated with ethical and authorized use of the internet and Government e-mail resources. Inappropriate use of such resources may result in disciplinary actions.

b. USU internet and e-mail users must use e-mail resources responsibly and abide by professional standards and conduct at all times.

c. The Cyber Security Officer must ensure that all IT staff are familiar with the policy and procedures contained herein and that possible criminal activity must be reported to the Cyber Security Officer immediately for further assessment and appropriate action. Where illegal activity is confirmed, the Departmental Director must be notified by the Cyber Security Manager.

4. Policies for using internet, e-mail, and monitoring of computer usage.

a. No expectation of privacy: The computers and computer accounts given to personnel are provided to assist them in the performance of their official duties. Personnel should not have any expectation of privacy in anything they create, store, send, or receive on the computer system.

b. No privacy in communications: Personnel should never consider electronic communications to be either private or secure. E-mail may be stored indefinitely on any number of computers, including that of the recipient. Copies of messages may be forwarded to others either electronically or on paper. In addition, e-mail sent to non-existent or incorrect usernames may be delivered to persons that you never intended.

c. Monitoring of computer usage: The Government has the right to monitor any and all aspects of its computer system, including, but not limited to, monitoring sites visited by personnel on the internet, monitoring chat groups and newsgroups, and reviewing material downloaded from, or uploaded to, the internet by users.

d. Blocking inappropriate content: The Government may use software to identify inappropriate internet sites. Such sites may be blocked from access by Government networks. In the event users encounter inappropriate or sexually explicit material while browsing on the internet, users are expected to immediately disconnect from the site, regardless of whether the site was subject to Government blocking software.

e. Prohibited activities: Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate may not be sent by e-mail or other form of electronic communication (bulletin board systems, newsgroups, chat groups), downloaded from the internet, or displayed on or stored in Government computers.

f. Viruses: Viruses can cause considerable damage to computer systems. Users should never download or accept e-mail attachments from unknown senders or use disks from outside sources without first scanning the material with USU-approved virus checking software. If a user suspects that a virus has been introduced into the Government's network, he or she must notify the USU Help Desk immediately for appropriate actions.

g. Reporting inappropriate activity: Users must submit complaints about inappropriate internet or e-mail activity to the Cyber Security Manager immediately. The Cyber Security Manager will inform a non-compliant user's immediate supervisor, who must consider disciplinary or other corrective actions, as appropriate. If potential criminal behavior is indicated, the Cyber Security Manager may be legally obligated to report such activity to the appropriate authorities with the concurrence and involvement of the CIO.

Non-compliance with this policy could result in loss of access to systems such as workstations, internet, e-mail, etc.

Enclosures:
1. References

REFERENCES

(a) DoDI 8500.01, "Cyber Security ," March 14, 2014

(b) DoDI 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997

Visitor Access Control and Common Access Card Inspection Program

1. Purpose.

In accordance with the provisions of the DoD Cyber Security Certification and Accreditation Process (DIACAP), USU Presidential Policy Memorandum (PPM) 15-2011, "Implementation of Visitor Access Control and Common Access Card (CAC) Inspection Program," establishes policies and procedures for monitoring visitor access throughout the campus and protection of network access utilities such as CAC.

2. References.

a. DoDI 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014.

b. USU-CIO Memorandum, DIACAP Traditional Security Review, July 22, 2011.

3. Applicability.

This policy applies to all USU students, faculty, and staff (military, civilian, and contractor).

4. Policy.

Establishes the policies and procedures as follows:

a. Common Access Card (CAC) Audit:

1) Per *reference (a)*, CACs must not be left unattended at any workstation to prevent security breaches.

2) The Cyber Security Division of the NOC and Security Department (SEC) will conduct joint monthly inspections to monitor compliance. Violations will be dealt with using a 3-tiered response as follows:

a) First violation: The Cyber Security team leaves a reminder card informing the user that his/her CAC was left unsecured along with a copy of the inspection memorandum.

b) Second violation: The Cyber Security team takes the CAC and leaves a note informing the user that the CAC has been turned in to SEC. Cyber Security and SEC will maintain a record of all CACs that have been turned in and claimed by respective owners.

c) Third violation: Same response as the second violation, to include supervisor notification for appropriate action.

3) CAC compliance issues will be included as an agenda item for Faculty Orientation briefings, Administrative Officers (AO) meetings, and Faculty Senate meetings.

b. Visitor access control and monitoring:

1) Sponsoring departments must escort visitors to SEC for badge issue and ensure an escort remains with the visitor while on campus.

2) Visitors must prominently display their badges for the duration of their visit.

3) Visitor sign in/out and badge turn-in process must be strictly enforced.

4) Staff members are encouraged to politely request visitors to show their badges if they are not visible.

5) Visitors requiring access to areas controlled by swipe card locks should be assisted by their sponsors to coordinate their visits with the respective departments. Visitors shall remain escorted during visits to such controlled areas.

5. Responsibilities.

a. The Cyber Security Manager shall ensure that a monthly CAC audit is conducted randomly. Reports shall be furnished to the CIO within three days of audit completion.

b. The Director of Security shall:

1) Maintain custody and responsibility for the CACs recovered during the audit. Logs will be maintained to account for CAC turn-in and retrieval by users.

2) Ensure enforcement of the visitor access control and monitoring and provide reports to the chain of command, as necessary.