

**BY ORDER OF THE  
SUPERINTENDENT**



**HQ UNITED STATES AIR FORCE  
ACADEMY INSTRUCTION 33-117**

**8 JANUARY 2013**

Certified Current on 9 May 2016  
**Communications and Information**

**USAFA INFORMATION TECHNOLOGY  
ENTERPRISE VULNERABILITY  
MANAGEMENT**

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**ACCESSIBILITY:** Publications and forms are available for downloading or ordering on the e-Publishing website at [www.e-publishing.af.mil](http://www.e-publishing.af.mil).

**RELEASABILITY:** There are no releasability restrictions on this publication.

---

OPR: USAFA/A6I

Certified by: USAFA/A6  
(Lt Col Gary Denney)

Pages: 11

---

This instruction implements Air Force Policy Directive (AFPD) 33-1, *Information Resources Management*. The purpose of this publication is to provide guidance for the protection of Enterprise Information Technology (IT) Systems on the United States Air Force Academy (USAFA). It includes USAFA policy for the USAFA Vulnerability Management Program to include Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) compliance, Information Assurance Vulnerability Alerts (IAVA), Notice to Airmen (C4 NOTAM), Time Compliance Network Order (TCNO), Time Compliance Technical Order (TCTO), Maintenance Task Order (MTO), Data Call Orders (DCO) and Network Tasking Order (NTO), and for the USAFA IT Enterprise. It also includes guidance for USAFA Incident Response, to include information system monitoring.

Guidance for IT Enterprise Vulnerability Management is addressed in several Federal, Department of Defense (DoD) and Air Force publications (see Attachment 1). All USAFA organizations and personnel will comply with this higher-level guidance unless exceptions or waivers are requested and approved as specified in this instruction. This instruction applies to all USAFA personnel. It does not apply to Air Force Reserve Command units or the Air National Guard. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using Air Force (AF) Form 847, *Recommendation for Change of Publication*. Ensure all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Information Management System (AFRIMS) Records Disposition Schedule located at <https://www.my.af.mil/afirms/afirms/afirms/rims.cfm>. The use of the name or mark of any

specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force. See Attachment 1 for a glossary of references and supporting information.

**1. USAFA Vulnerability Management Program.** The DoD Information Assurance Vulnerability Management (IAVM) Program is an enterprise-wide program to address security of information systems supporting the academic mission. The goals of the DoD IAVM Program are to identify & mitigate network vulnerabilities posing threats to DoD systems and information, improve Configuration Management and provide situational awareness across the Global Information Grid. The USAFA Vulnerability Management Program Policy describes the roles and responsibilities of organizations and personnel required to comply with, track and report vulnerability mitigation. The following are the organizational roles and responsibilities

1.1. DoD High-Performance Computing Modernization Office (HPCMO) is:

1.1.1. The Computer Network Defense Service Provider (CNDSP) for the Defense Research and Engineering Network (DREN), which includes .EDU and ResearchNet. As the CNDSP for DREN, HPCMO monitors all .EDU and ResearchNet systems and assets, and provides direction for DoD IAVM compliance. The HPCMO defines “assets” as any device on DoD owned, controlled or contracted information system or network (e.g., workstations, servers switches, routers, firewalls, network peripherals, portable electronic devices, or controlled interfaces).

1.1.2. Responsible for using United States Cyber Command (USCYBERCOM) IAVAs and other identified vulnerability-related configuration requirements to disseminate vulnerability notices, and provide direction to High Performance Computing (HPC) users (including 10th Communications Squadron (10 CS) for .EDU and the ResearchNet Administrator).

1.1.3. Responsible for tracking acknowledgement and compliance responses, oversees Plan of Action and Milestones (POAM) related to IAVA implementation, scans for IAVM compliance validation, and provides guidance and/or technical assistance as needed.

1.1.4. The Maintainer of a monthly watch list for senior leadership that highlights significant issues resulting from IAVM noncompliance. These issues include failure to report IAVA compliance, incidents resulting from exploitation of an IAVA vulnerability, noncompliant assets identified by outside scans, audits, or inspections, missing or incomplete POAMs, and a pattern of organization IAVM noncompliance and/or failure to identify causes and take corrective action.

1.2. USAFA Director of Communications and Information (HQ USAFA/A6) will:

1.2.1. Collect metrics from 10 CS and ResearchNet to present a monthly report to the USAFA/CC In Accordance With (IAW) the USAFA IT Enterprise Vulnerability Management Plan.

1.2.2. Establish policy and guidelines.

1.3. 10 CS will:

1.3.1. Update and maintain the USAFA IT Enterprise Vulnerability Management Plan (VMP) and file it as part of the 10 CS IT Service Catalog.

1.3.1.1. The VMP will address vulnerability management reporting and compliance requirements to include a reporting matrix for all networks in the USAFA IT Enterprise. The VMP will detail monthly metric requirements for vulnerability management compliance and situational awareness (e.g., Information Assurance (IA) Workforce Training compliance, Federal Information Security Management Act compliance, STIG Compliance, Host-Based Security System (HBSS) results, Penetration Attempts, numbers of Category I, II, III and IV vulnerabilities on the USAFA networks, etc.).

1.3.2. Ensure all systems (with associated network devices) on .EDU and .MIL networks have Information Assurance Officers (IAO)/Functional Systems Administrators (FSA) assigned and appointed in writing by their Mission Partners (MP) or units. In addition to IAOs and FSAs, the .EDU network systems are required to have Client System Technicians (CST) assigned. A list of all CSTs/IAOs/FSAs will be maintained on the 10 CS SharePoint site and will be revalidated annually. The Wing Information Assurance Manager (IAM) will receive a copy of the list and appointment letters.

1.3.3. Serve as the wing/base OPR to acknowledge, disseminate, implement, track and report compliance with STIGs, TCNOs and C4 NOTAMs on the .MIL network IAW the USAFA IT Enterprise Vulnerability Management Plan. In this capacity, 10 CS will:

1.3.3.1. Follow 561st Network Operations Squadron (561 NOS) direction for any local implementation requirements for devices on the .MIL network.

1.3.3.2. Implement TCNOs and C4 NOTAMs, and track, compile, assess, and report TCNO compliance, extensions, and situational awareness metrics for all .MIL systems and associated network devices IAW AFI 33-138, *Enterprise Network Operations and Tracking*, and 690th Network Support Group (690 NSG) SPIN-1.

1.3.3.3. Ensure compliance with applicable DISA STIGs for all USAFA networks.

1.3.4. Serve as the wing/base OPR to implement the VMP for the .EDU enclave and core services. In this capacity, 10 CS will:

1.3.4.1. Scan the .EDU enclave and core services monthly for vulnerabilities/compliance and upload scan results into Vulnerability Management Systems (VMS) and eRetina Server on a monthly basis. HPCMO and 10 CS IAOs/IAMs will have access to VMS and eRetina Servers to track vulnerability mitigation progress. 10 CS will provide scan results to organizational IAOs for review and mitigation.

1.3.4.2. Mitigate all Category (CAT) I vulnerabilities IAW STIG and IAVA requirements on the .EDU enclave and core services.

1.3.4.3. Mitigate all CAT II and CAT III vulnerabilities IAW DoD 8500.2, *IA Implementation*, DoD 8510.01, *DoD Information Assurance Certification and Accreditation Process (DIACAP)*, DISA STIGs, and IAVA requirements. Exceptions or variance requests can be submitted for CAT III findings/vulnerabilities through the IT Change Management process IAW USAFAI 33-116, *USAFA IT Change*

*Management.* Exceptions and variances approved by the Change Advisory Board (CAB) will be coordinated through the Wing IAM and USAFA/A6 to be included as artifacts in the applicable Authority To Operate (ATO) package in Enterprise Mission Assurance Support Service for the Designating Accrediting Authority's approval. The Wing IA Office will record and track all approved IAVA exceptions, variances, or mitigations and submit to HPCMO.

1.3.4.4. Track, compile, assess and report STIG and IAVA compliance for the .EDU enclave and core services IAW HPCMO direction and the USAFA IT Enterprise Vulnerability Management Plan. Collect and consolidate vulnerability management reports from .EDU for submission to HPCMO as required.

1.3.4.5. Review all IAVAs generated by the HPCMO for implementation and evaluate for feasibility on the .EDU enclave and core services. The 10 CS/SCO will provide recommendations for application on the .EDU to the CAB. The 10 CS/SCO will implement IAVAs on .EDU enclave and core services only after CAB approval. 10 CS will task FSAs to implement all approved IAVAs onto FSA-owned systems within 21 working days of CAB approval. If not implemented 10 CS Wing IA office will notify system FSAs, organizational leadership and 10 CS leadership that the system will be turned off for non-compliance. The FSA-owned system will not be returned to the network until the system FSA, and 10 CS/SCO have confirmed to Wing IA that the system has been remediated. For further detail reference Vulnerability Notice Timeline Memorandum for Record, dated 4 September 2012.

1.3.4.6. Conduct assessments on .EDU IAW AFI 33-230, *Information Assurance Assessment and Assistance Program*.

1.3.5. Ensure CSTs/IAOs/FSAs meet IA certification requirements IAW DoD 8570.01-M, *Information Assurance Workforce Improvement Program*, AFMAN 33-285, *Information Assurance (IA) Workforce Improvement Program*, and USAFAI 33-118, *Communications and Information*.

1.4. ResearchNet Administrator will:

1.4.1. Be the Vulnerability Management OPR for ResearchNet.

1.4.2. Ensure all systems (with associated network devices) on ResearchNet have CSTs/IAOs/FSAs assigned and appointed in writing. A list of all CSTs/IAOs/FSAs will be maintained by the ResearchNet Administrator and will be revalidated annually. The Wing IAM will receive a copy of the list and appointment letters.

1.4.3. Mitigate all CAT I vulnerabilities IAW STIG and IAVA requirements on the ResearchNet enclave and core services.

1.4.3.1. Mitigate all CAT II and CAT III vulnerabilities IAW DoD 8500.2, DoD 8510.01, DISA STIGs, and IAVA requirements. Exceptions or variance requests can be submitted for CAT III findings/vulnerabilities through the IT Change Management process IAW USAFAI 33-116, *USAFA IT Change Management*. Exceptions and variances approved by the CAB will be coordinated through the Wing IAM and USAFA/A6 to be included as artifacts in the applicable ATO package in Enterprise Mission Assurance Support Service for Designating Accrediting Authority approval.

The Wing IA Office will record and track all approved IAVA exceptions, variances, or mitigations and submit to HPCMO.

1.4.4. Track, compile, assess and report STIG and IAVA compliance for the ResearchNet enclave and core services IAW HPCMO direction and the USAFA IT Enterprise Vulnerability Management Plan. All ResearchNet IAVA reports must be submitted to HPCMO and copies sent to the 10 CS Communication Focal Point (CFP) IAW Technical Order 00-33A-1001, *General Communications Activities Management Procedures and Practice Requirements* and AFI 33-138.

1.4.5. Scan the ResearchNet enclave and core services monthly for vulnerabilities/compliance and upload scan results into VMS and eRetina Server on a monthly basis. HPCMO, IAOs/IAMs will have access to VMS and eRetina Servers to track vulnerability mitigation progress.

1.5. MPs and units will:

1.5.1. Ensure CSTs/IAOs/FSAs are appointed in writing for their functional community of interest systems, servers, workstations, peripherals, communications devices, and software. Devices and systems that do not connect to, or exchange data with, systems or devices on DoD-provisioned networks are exempt from this requirement (e.g., stand-alone laboratory networks, etc.).

1.5.2. Ensure CSTs/IAOs/FSAs meet IA certification requirements IAW DoD 8570.01-M, AFMAN 33-285 and USAFAI 33-118.

1.6. FSAs will:

1.6.1. Ensure their functional communities of interest systems, servers, workstations, peripherals, communications devices, and software are on-line and supported IAW AFI 33-115V1, *Network Operations (NETOPS)*, paragraph 4.6. and perform Vulnerability Management duties for their respective networks, systems and assets.

1.6.2. Meet IA certification requirements IAW DoD 8570.01-M, AFMAN 33-285 and USAFAI 33-118. The CSTs/FSAs must meet IA certification requirements IAW DoD 8570.01-M, AFMAN 33-285 and USAFAI 33-118.

1.6.3. Meet requirements IAW Memorandum for Record, *Vulnerability Notice Timeline*, dated 4 September 2012.

1.6.4. Mitigate all CAT I, vulnerabilities IAW STIG and IAVA requirements on their respective networks, systems, and assets within 21 days.

1.6.4.1. Mitigate all CAT II and CAT III vulnerabilities IAW DoD 8500.2, DoD 8510.01, DISA STIGs, and IAVA requirements. Exceptions or variance requests can be submitted for CAT III findings/vulnerabilities through the IT Change Management process IAW USAFAI 33-116. Exceptions and variances approved by the CAB will be coordinated through the Wing IAM and USAFA/A6 to be included as artifacts in the applicable ATO package in Enterprise Mission Assurance Support Service for Designating Accrediting Authority approval. The Wing IA Office will record and track all approved IAVA exceptions, variances, or mitigations and submit to HPCMO.

1.6.5. Track, compile, assess, and report STIG and IAVA compliance for their respective networks IAW the USAFA IT Enterprise Vulnerability Management Plan. All Vulnerability Management reporting must be submitted to the Wing IA Office.

1.6.6. Acquire a Remedy Account from 10 CS.

**2. USAFA Incident Response Policy.** The USAFA Incident Response Policy describes the roles and responsibilities of organizations and personnel required to respond to incidents on USAFA networks. The following are the organizational roles and responsibilities:

2.1. 10 CS will:

2.1.1. Be responsible for Incident Response on the USAFA IT Enterprise

2.1.2. Monitor .EDU systems to detect and react to incidents, intrusions, disruption of services, or other unauthorized activities.

2.1.3. Develop and maintain a USAFA IT Enterprise Incident Response Plan (IRP) to prepare for potential incidents.

2.1.3.1. The IRP will identify Incident Response Team members to include representatives from Wing IA and NetOps. Depending on the severity, an incident notification may include Information Protection, Office of Special Investigations, Judge Advocate, and Public Affairs.

2.1.3.2. The IRP will address Incident Identification to include symptoms and indications, scope and monitoring/follow-up.

2.1.3.3. The IRP will address Incident Handling Processes for specific incident types (i.e., Classified Message Incidents, intrusions).

2.1.4. Develop Incident Handling Procedures to include quick-reaction checklists to be used during an incident.

2.1.5. Respond, contain and/or eliminate potential incidents once they have been identified.

2.1.5.1. IAW AFI 33-138, paragraph 2.8.3.1., oversee and orchestrate vulnerability, security incident, and intrusion response actions whenever an incident affects the .EDU, .MIL (when applicable), ResearchNet, or other IT resources.

2.1.5.2. IAW AFI 33-138, paragraph 2.8.3.2., assist users in eradicating malicious logic and other incidents from networks, information systems, and stand-alone computing devices.

2.1.5.3. Authorized to terminate network services and isolate offending networks or systems until an incident is resolved.

2.1.6. Ensure documentation is collected during the incident to allow for proper reporting, to facilitate potential forensics analysis and to review actions taken for appropriateness. IAW AFI 33-138, paragraph 2.8.3.3, assist users in assessing the scope of unauthorized network activities and incidents.

2.1.7. Incident Reporting:

- 2.1.7.1. IAW AFI 33-138, paragraph 2.8.3.5., maintain USAFA IT situational awareness by tracking, compiling, and reporting USAFA statistics on unauthorized network activity and incidents.
- 2.1.7.2. IAW AFI 33-138, paragraph 2.8.3.4., report to the 561 NOS all unauthorized activities and incidents that occur on the .MIL network under 10 CS/SCO purview. Incident reporting will follow guidelines established in the Incident Response Plan.
- 2.1.8. Ensure all devices on USAFA networks have DoD HBSS installed and properly configured to ensure adequate monitoring.
- 2.2. ResearchNet Administrator will:
  - 2.2.1. Report incidents to the HPCMO and the CFP/USAFA IT Service Desk for resolution IAW AFMAN 33-152, *User Responsibilities and Guidance for Information Systems*.
  - 2.2.2. Ensure all devices on ResearchNet have DoD HBSS installed and properly configured to ensure adequate monitoring HPCMO.
- 2.3. USAFA IT Users will:
  - 2.3.1. Report all security incidents to their organization IAO.
- 2.4. IAO/FSA/CSTs will:
  - 2.4.1. Report security incidents to the CFP/USAFA IT Service Desk for resolution IAW AFMAN 33-152.

MICHAEL C. GOULD, Lt Gen, USAF  
Superintendent

**Attachment 1****GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

CJCSI 6211.02, *Defense Information Systems Network (DISN): Policy and Responsibilities*  
CJCSI 6510.01F, *Information Assurance (IA) and Support to Computer Network Defense (CND)*  
DoD 8570.01-M, *Information Assurance Workforce Improvement Program*  
DoDD 8500.01E, *Information Assurance (IA)*  
DoDD O-8530.1, *Computer Network Defense (CND)*  
DoDI 8500.2, *Information Assurance (IA) Implementation*  
DoDI O-8530.2, *Support to Computer Network Defense (CND)*  
DoDI 8560.01, *Communications Security (COMSEC) Monitoring and Information Assurance (IA) Readiness Testing*  
AFPD 33-2, *Information Assurance (IA) Program*  
AFI 33-115V1, *Network Operations (NETOPS)*  
AFI 33-115V2, *Licensing Network Users and Certifying Network Professionals*  
AFI 33-138, *Enterprise Network Operations Notification and Tracking*  
AFI 33-200, *Information Assurance (IA) Management*  
AFI 33-201V1, *Communications Security (COMSEC)*  
AFI 33-201V2 *Communications Security (COMSEC) User Requirements*  
AFI 33-210, *Air Force Certification and Accreditation (C&A) Program (AFCAP)*  
AFI 33-230, *Information Assurance Assessment and Assistance Program*  
AFMAN 33-285, *Information Assurance (IA) Workforce Improvement Program*  
690th Network Support Group (690 NSG) Special Instruction-1 (SPIN-1)  
DISA Security Technical Implementation Guides (STIG)  
USAFAI 33-116, *Information Technology Change Management*

***Adopted Forms***

AF Form 847, *Recommendation for Change of Publication*, 22 September 2009

***Abbreviations and Acronyms***

**AF**—Air Force

**AFI**—Air Force Instruction

**AFMAN**—Air Force Manual

**AFPD**—Air Force Policy Directive

**AFRIMS**—Air Force Records Information Management System

**ATO**—Authority To Operate

**CAB**—Change Advisory Board

**CAT**—Category

**CFP**—Communications Focal Point

**CNDSP**—Computer Network Defense Service Provider

**COMSEC**—Communication Security

**CS**—Communications Squadron

**CST**—Client System Technician

**DCO**—Data Call Orders

**DISA**—Defense Information Systems Agency

**DISN**—Defense Information System Network

**DREN**—Defense Research and Engineering Network

**DoD**—Department of Defense

**DoDD**—Department of Defense Directive

**FSA**—Functional System Administrator

**HBSS**—Host-Base Security System

**HPC**—High-Performance Computing

**HPCMO**—High-Performance Computing Modernization Office

**IA**—Information Assurance

**IAM**—Information Assurance Manager

**IAO**—Information Assurance Officer

**IAVA**—Information Assurance Vulnerability Alert

**IAVM**—Information Assurance Vulnerability Management

**INOSC**—Integrated Network Operations and Security Centers

**IRP**—Incident Response Plan

**IT**—Information Technology

**MP**—Mission Partner

**MTO**—Maintenance Task Order

**NOS**—Network Operations Squadron

**NOTAM**—Notice to Airmen

**NSG**—Network Support Group

**NTO**—Network Tasking Order

**OPR**—Office of Primary Responsibility

**POAM**—Plan of Action and Milestones

**SCO**—Network Operations

**SPIN**—1—Special Instruction

**STIG**—Security Technical Implementation Guide

**TCNO**—Time Compliance Network Order

**TCTO**—Time Compliance Technical Order

**USAFA**—United States Air Force Academy

**USCYBERCOM**—United States Cyber Command

**VMS**—Vulnerability Management System

**VMP**—Vulnerability Management Plan

### *Terms*

**DISA**—In addition to other services offered, DISA develops and provides security configuration guidance for IA and IA-enabled IT products. The guidelines are outlined in DISA's STIG, which identify existing and potential vulnerabilities on a system. STIGS exist for a variety of operating systems and applications. Within each STIG, DISA defines four vulnerability codes from CAT I (high vulnerability) to CAT IV (low vulnerability):

**CAT I**—Vulnerabilities that allow an attacker immediate access into a machine, allow super user access, or bypass a firewall.

**CAT II**—Vulnerabilities that provide information that has a high potential of giving access to an intruder.

**CAT III**—Vulnerabilities that provide information that potentially could lead to compromise.

**CAT IV**—Vulnerabilities that provide information that will lead to the possibility of degraded security.

**USCYBERCOM**—Plans, coordinates, integrates, synchronizes, and conducts activities to: direct the operations and defense of specified DoD information networks and; prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries. The USCYBERCOM manages the DoD IAVM program and issues IAVAs to provide computer application software or operating system vulnerability notification in the form of alerts, bulletins, and technical advisories.

**24th Air Force**—The operational warfighting organization that establishes, operates, maintains and defends Air Force networks and conducts full-spectrum operations in cyberspace. The 24th Air Force provides full-spectrum management and defense for AF Network Operations through the 67th Network Warfare Wing, the 690th NSG.

**561 Network Operation Squadron**—Operates one of two INOSCs for 690 NSG. The INOSC is the CNDSP for Air Force Information Systems including, but not limited to NIPRNet and SIPRNet.

**IAVA A (Alert)**—An IAVA A is a vulnerability defined as severe, having potential to critically impact DoD systems and information. The IAVA As require acknowledgement and compliance responses, and a Plan of Action and Milestones (POAM) is required for noncompliance.

**IAVA B (Bulletin)**—An IAVA B is a vulnerability which does not pose an immediate risk to DoD systems, but is significant enough that noncompliance without corrective action could escalate the risk. The IAVA Bs require acknowledgement response. The HPC sites must be in compliance with IAVA B notices.

**IAVA T (Technical Advisory)**—An IAVA T advises that a vulnerability exists but is generally categorized as low risk. No acknowledgement or compliance response is required.