DoD Instruction 8531.01

DoD Vulnerability Management

Originating Component:	Office of the DoD Chief Information Officer
Effective:	September 15, 2020
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Approved by:	Dana Deasy, DoD Chief Information Officer

Purpose: In accordance with the authority in DoD Directive 5144.02, this issuance:

- Establishes policy, assigns responsibilities, and provides procedures for DoD vulnerability management and response to vulnerabilities identified in all software, firmware, and hardware within the DoD information network (DODIN).
- Establishes a uniform DoD Component-level cybersecurity vulnerability management program based on federal and DoD standards.
- Establishes policy and assigns responsibilities for the DoD Vulnerability Disclosure Program (VDP).
- Establishes policy, assigns responsibilities, and provides procedures for DoD's participation in the Vulnerabilities Equities Process (VEP), in accordance with the Vulnerabilities Equities Policy and Process for the U.S. Government (USG).

TABLE OF CONTENTS

TABLES

FIGURES

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

This issuance applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this issuance as the "DoD Components").

1.2. POLICY.

The DoD will:

a. Use the DoD vulnerability management process to manage and respond to vulnerabilities identified in all software, firmware, and hardware within the DODIN.

b. Ensure configuration, asset, remediation, and mitigation management supports vulnerability management within the DODIN in accordance with DoD Instruction (DoDI) 8510.01.

c. Support all systems, subsystems, and system components owned by or operated on behalf of DoD with efficient vulnerability assessment techniques, procedures, and capabilities. In leased systems, enforcement is included in contract language to mitigate vulnerabilities consistent with DoD policies.

d. Maintain the requirements for DoD participation in the VEP and ensure DoD and OSD Components submit a vulnerability to the VEP that is both a newly discovered vulnerability and not publicly known vulnerability, as soon as practicable.

e. Develop and maintain a coordinated VDP.

SECTION 2: RESPONSIBILITIES

2.1. DOD SENIOR INFORMATION SECURITY OFFICER (DOD SISO).

Under the authority, direction, and control of the DoD Chief Information Officer, the DoD SISO:

a. Develops policy and guidance for the management of cybersecurity vulnerabilities.

b. Ensures DoD Information Security Continuous Monitoring capability incorporates information from vulnerability management activities and capabilities.

c. Establishes guidance on the frequency of configuration compliance checks.

d. Specifies methodologies, metrics, and collection capabilities for DoD Components to measure the effectiveness of and compliance with DoD Component vulnerability management processes.

e. Oversees software, firmware, and hardware vulnerability management, automated patch management, and compliance auditing capabilities (e.g., DoD established technical capabilities) developed for the DoD enterprise.

f. Provides policy and guidance for the DoD Cyber Crime Center (DC3), oversees operations in accordance with the VDP and integrates critical VDP metrics into compliance reporting to provide accountability for remediation and mitigation of discovered vulnerabilities.

g. Coordinates with the National Institute of Standards and Technology (NIST) in the development of vulnerability management standards and guidelines in collaboration with the Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS).

h. Provides one or more subject matter expert (SME) to support equities determinations and discussions for the VEP as needed.

i. Integrates key VDP metrics into the DoD Cybersecurity Scorecard.

2.2. DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (DISA).

Under the authority, direction, and control of the DoD Chief Information Officer, and in addition to the responsibilities in Paragraph 2.10., the Director, DISA:

a. Maintains the Defense Asset Distribution Systems DoD Patch Repository.

(1) Provides access on major DoD enterprise networks to patches for DoD-approved software used by DoD systems or devices that can be automatically leveraged by automated patching services, where possible, or manually downloaded and applied, when necessary.

(2) Tests and verifies patch source and integrity to ensure the patch is valid and is not maliciously or accidentally altered.

b. Acquires and develops capabilities, standards, and integration frameworks for vulnerability management, asset management, configuration management, and remediation or mitigation management.

c. Maintains a list of available enterprise-designated automated vulnerability management capabilities approved for DoD Components' use.

d. Develops security technical implementation guides and security requirements guides for information systems, networks, and devices.

e. Establishes contracts and non-disclosure agreements or memorandums of agreement with vendors for systems, system components, and devices used across the DoD to:

(1) Facilitate the exchange of vulnerability management-related information.

(2) Validate and measure compliance with current DoD vulnerability management-related direction through an automated process.

(3) Authorize hosting and distribution of software, firmware, and patches for licensed and copyrighted products.

f. Provides operational concepts and guides for the DoD Components' use of all DISA-provided vulnerability management systems and capabilities.

g. Maintains the Continuous Monitoring Risk Scoring System.

h. Coordinates any DoD vulnerability management, asset management, configuration management, and remediation or mitigation management issues or concerns with Commander, United States Cyber Command (USCYBERCOM), and Joint Force Headquarters-DoD Information Network (JFHQ-DODIN).

i. When vendor-provided security hardening guidance is insufficient for DoD's security needs, develops cybersecurity configuration guidance pursuant to DoDI 8500.01 and Committee on National Security Systems Instruction (CNSSI) No. 1253 in collaboration with the DIRNSA/CHCSS.

2.3. UNDER SECRETARY OF DEFENSE FOR AQUISITION AND SUSTAINMENT (USD(A&S)).

The USD(A&S):

a. Identifies, develops, updates, and implements policy and processes for the DoD acquisition contracting process for software maintenance and sustainment support to ensure:

(1) Consistency and coherence of vulnerability assessment across systems and their interfaces.

(2) Secure configuration and active responsiveness to vulnerability remediation and mitigation actions within DoD-approved programs throughout the life cycle of the program.

(3) Secure software development and reduction of software vulnerabilities to new and existing software by planning for near real-time software vulnerability identification and regularly scheduled patch cycles.

b. Ensures acquisition policy includes requirements for the identification, planning, and replacement of unsupported software, firmware, and hardware during a system's life cycle and the identification of developed software components (e.g., executable programs) installed on DoD devices in accordance with DoDI 5000.02T.

c. Incorporates security assurance checks into procurement and acquisition policy to reduce DoD risk associated with malign use of the product or products.

d. Provides guidance for the management of software, hardware, and firmware vulnerabilities through the Defense Federal Acquisition Regulation and any supporting Defense Federal Acquisition Regulation Supplement, and through other applicable government acquisition policies and guidelines.

e. Provides one or more SMEs to support equities determinations and discussions for the VEP as needed.

2.4. UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING.

The Under Secretary of Defense for Research and Engineering:

a. Provides one or more SMEs to support equities determinations and discussions for the VEP as needed.

b. Provides oversight of the Federally Funded Research and Development Centers, National Laboratories, and University Affiliated Research Centers, to ensure they report qualified vulnerabilities to the VEP when discovered in a DoD-sponsored project, in coordination with USD(A&S).

c. Notifies the Under Secretary of Defense for Policy (USD(P)) VEP point of contact of any applicable vulnerabilities identified during cyber incident damage assessments carried out by or reported to the OSD Damage Assessment Management Office.

d. Ensures the OSD Damage Assessment Management Office provides cybersecurity vulnerability damage assessments.

e. Maintains the DoD Joint Federated Assurance Center to:

(1) Support defense system requirements.

(2) Ensure the security of software and hardware developed, acquired, maintained, and used by the DoD.

2.5. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY (USD(I&S)).

The USD(I&S):

a. Coordinates with DoD SISO on security policy and related intelligence and security matters for safeguarding information on systems and networks.

b. Provides one or more SMEs to support equities determinations and discussions for the VEP as needed.

c. Approves or denies requests for public disclosure of VDP vulnerabilities in coordination with the USD(P) and DC3.

2.6. DIRNSA/CHCSS.

Under the authority, direction, and control of the USD(I&S), and in addition to the responsibilities in Paragraph 2.10., the DIRNSA/CHCSS:

a. Assesses the overall security posture of all DoD systems and disseminates information on threats and vulnerabilities impacting DoD system components in coordination with USCYBERCOM.

b. Provides cybersecurity support to DoD Components to assess vulnerabilities and establish security implementation specifications and, in collaboration with DISA, develops security technical implementation guides.

c. Identifies, monitors, and analyzes vulnerabilities of software, firmware, and hardware used by DoD.

d. Serves as the VEP Executive Secretariat (ES).

e. Serves as one of four DoD representatives for the VEP to the National Security Council staff for interagency meetings, such as the Equities Review Board (ERB) as established in the Vulnerabilities Equities Policy and Process for the USG, and additional department-level activities.

f. Designates a VEP point of contact to serve both as the focal point for vulnerability submissions from National Security Agency (NSA) to the VEP and the primary contact for NSA for communication and coordination with the VEP ES.

g. Manages risk assessments, mitigation processes, and timelines for remediating vulnerabilities found in cryptographic government-off-the-shelf equipment, systems certified by NSA/Central Security Service (CSS), or vulnerabilities discovered in any cryptographic function, whether in hardware, firmware, or software approved by NSA/CSS. Submit those vulnerabilities to the VEP as applicable.

2.7. DIRECTOR, DEFENSE HEALTH AGENCY.

Under the authority, direction, and control of the Under Secretary of Defense for Personnel and Readiness, through the Assistant Secretary of Defense for Health Affairs, and in addition to the responsibilities in Paragraph 2.10., the Director, Defense Health Agency, in accordance with DoDI 6530.01:

a. Exercises oversight for the management of software, firmware, and hardware vulnerabilities within DoD medical systems and devices.

b. Provides additional specialized guidance, as required, for DoD medical devices in accordance with FDA-2015-D-5105 and FDA-2013-S-0610.

2.8. USD(P).

The USD(P):

a. Ensures the development of VDP's scope and activities are consistent to improve relations with the security researcher community.

b. Ensures VDP is transparent to the public.

c. Coordinates and approves any requested changes to the VDP scope.

d. Approves or denies requests for public disclosure of VDP vulnerabilities in coordination with the USD(I&S) and DC3.

e. Serves as the primary DoD representative for the VEP to the National Security Council staff for interagency meetings, such as the ERB, and additional department-level activities.

f. Designates a VEP point of contact to serve as the focal point for vulnerability submissions from OSD components to the VEP and the primary OSD contact for communication and coordination with the VEP ES.

g. Appoints SMEs from DoD Components to support equities determinations and discussions for the VEP as needed.

2.9. UNDER SECRETARY OF DEFENSE (COMPTROLLER)/CHIEF FINANCIAL OFFICER, DEPARTMENT OF DEFENSE.

The Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense:

a. Exercises oversight for the management of software and hardware vulnerabilities within financially-significant systems and applications.

b. Provides additional specialized guidance, as required, for financial improvement and audit readiness controls in accordance with the guidance in the Federal Information Systems Controls Audit Manual.

2.10. DOD COMPONENT HEADS.

The DoD Component heads:

a. Establish the DoD Vulnerability Management Process through a vulnerability management program for systems, subsystems, and system components.

b. Establish asset management, configuration management, and remediation and mitigation programs to support their vulnerability management process.

c. Designate the organizations responsible for directing and managing the vulnerability management program and coordinating with JFHQ-DODIN.

d. Coordinate all vulnerability reports and assessments with USCYBERCOM/JFHQ-DODIN as required.

e. Create a DoD Component-level or Service-level prioritization and scheduling plan for the deployment of patches, updates, configuration changes, hardware upgrades, or directed actions to remediate vulnerabilities.

f. Track and report mitigations and risk acceptance status to JFHQ-DODIN.

g. Request assistance, as needed, from the Joint Federated Assurance Center in the establishment of vulnerability management programs, vulnerability tracking and reporting, and the incorporation of software, firmware, and hardware vulnerability analysis capabilities.

h. Establish and provide guidance to system owners and program managers on mitigation deployment, DoD Component risk tolerance, and designated authority to accept risk.

i. Implement patches, upgrades, and other remediation or mitigation actions directed by the Commander, USCYBERCOM, through JFHQ-DODIN, and as applicable based on network/system scans.

j. Identify and provide guidance on security-relevant configurations for DoD Component software, firmware, and hardware.

k. Determine and communicate requirements for mitigations by the system owner, program manager, or other DoD Component organizations.

l. Account for all software, firmware, and hardware items used on systems, system components, and devices owned or operated on behalf of the DoD Component; maintain current inventory in DoD information technology asset management systems.

m. Ensure DoD Component conducts audits for patching, compliance, and reporting.

n. Ensure DoD Component creates and uses unique item identifiers and automated systems for software, firmware, and hardware items in accordance with DoDI 8320.03 and 8320.04.

o. Provide SMEs to support equities determinations and discussions for the VEP as needed.

2.11. SECRETARY OF THE AIR FORCE.

In addition to the responsibilities in Paragraph 2.10., the Secretary of the Air Force, through the Director, DC3:

a. Manages the DoD's VDP public engagement efforts.

b. Functions as the single focal point for receiving vulnerability reports and interacting with researchers supporting the VDP.

c. Coordinates with JFHQ-DODIN to ensure the delivery of reports to the system's owner and helping the remediation team as quickly as possible.

d. Coordinates and gains approval from USCYBERCOM/JFHQ-DODIN before releasing requests by researchers for the public disclosure of vulnerabilities according to the policy and procedures approved by the USD(P) and Assistant to the Secretary of Defense for Public Affairs, and the USD(I&S) as appropriate.

e. Coordinates with JFHQ-DODIN to ensure vulnerabilities discovered as part of the VDP are considered for submission through USCYBERCOM to the VEP.

f. Operates, maintains, and provides user training for the Vulnerability Report Management Network (VRMN) platform for use by DC3, JFHQ-DODIN, and the components.

g. Serves as one of four DoD representatives for VEP to the National Security Council staff for interagency meetings, such as the ERB.

h. Designates a VEP point of contact to serve as the focal point for vulnerability submissions from DC3 to the VEP for coordination with the VEP ES.

i. Disseminates remediation and mitigation options-approved through the VEP to the Defense Industrial Base.

2.12. CJCS.

In addition to responsibilities in Paragraph 2.10., the CJCS:

a. Manages military support to the VEP and oversees the execution of USCYBERCOM's roles and responsibilities for the VEP.

b. Ensures that joint equities and the potential impact of vulnerabilities on joint operations are represented in VEP submissions to USCYBERCOM, in coordination with the Combatant Commands.

c. Coordinates internal reviews of DoD and interagency VEP submissions with the Combatant Commands and Military Departments.

d. Coordinates vulnerability submissions from the Combatant Commands to USCYBERCOM for review and submission to the VEP.

2.13. COMMANDER, USCYBERCOM.

In addition to the responsibilities in Paragraph 2.10., the Commander, USCYBERCOM:

a. Establishes and assigns responsibilities for managing DoD-wide vulnerabilities through JFHQ-DODIN.

(1) Establishes procedures to direct and track implementation of patches, updates, configuration changes, hardware upgrades, and other remediation or mitigation actions.

(2) Directs and prioritizes specific measures to remediate or mitigate software, firmware, and hardware vulnerabilities and threat activities, including disconnection from DODIN transport services, under assigned directive authority for cyberspace operations.

(3) Distributes or produces orders and directives to DoD Components to mitigate or prevent the risk of threats exploiting vulnerabilities.

(4) Oversees DoD Component implementation and reporting on directed vulnerability management actions.

(5) Manages operational risk for systems, subsystems, and system components operating or connected to the DODIN.

(6) Receives VDP reports from DC3 and directs actions to mitigate and remediate vulnerabilities within the VRMN platform. The VRMN is located at: https://vrmn.dc3.smil.mil.

(7) Appoints SMEs to support equities determinations and discussions for the VEP as needed.

b. Establishes an office to serve as the primary DoD focal point for receiving and processing all vulnerability submissions from DoD to the VEP in coordination with the CJCS and the USD(P).

c. Serves as one of four DoD representatives for VEP to the National Security Council staff for interagency meetings, such as the ERB and additional department-level activities.

d. Designates a VEP point of contact to serve as the focal point for vulnerability submissions from USCYBERCOM to the VEP ES for communication and coordination.

e. Coordinates with the CJCS and the USD(P) to review vulnerabilities and submit them to the VEP.

f. Assists DoD Components to develop, maintain, and update mitigation plans and recommend mitigation options and deployment plans for vulnerabilities submitted to the VEP.

g. Coordinates with the U.S. Computer Emergency Readiness Team (US-CERT), the CERT Coordination Center, and the United States Intelligence Community Security Coordination Center for cyber threat updates.

h. Shares information about vulnerabilities with the DoD US-CERT liaison in accordance with Section 3556 of Title 44, United States Code, also known and referred to in this issuance as the "Federal Information Security Modernization Act of 2014."

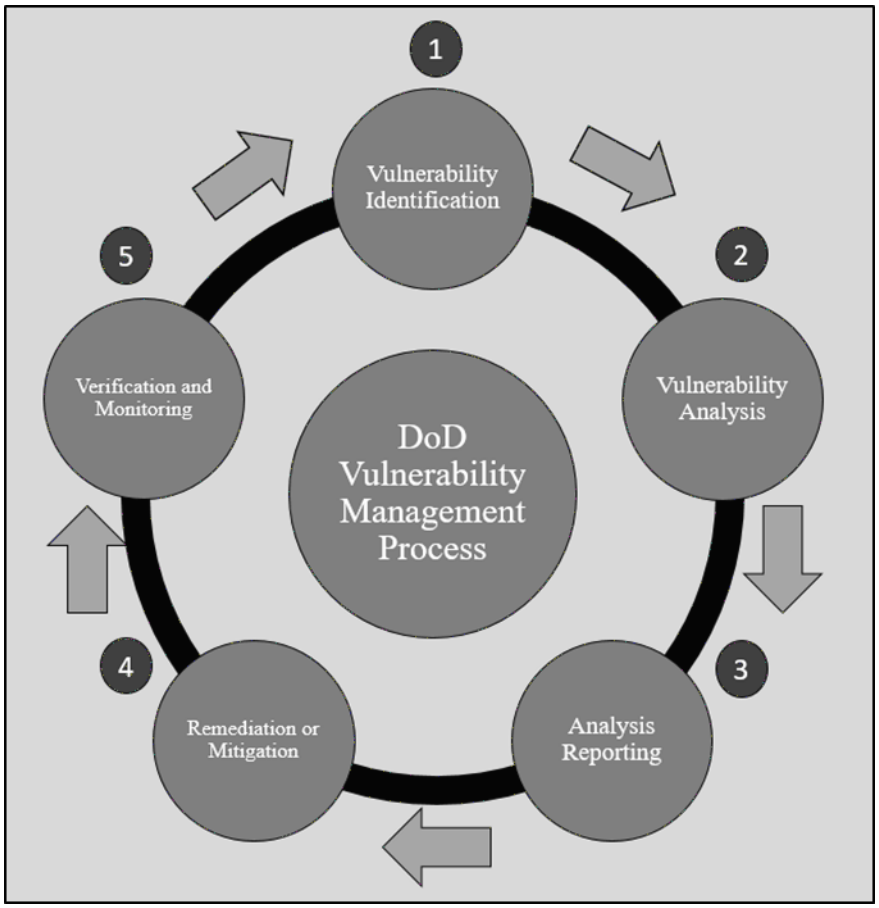
i. Coordinates with the US-CERT to identify potential remediation and mitigation actions as required.

SECTION 3: VULNERABILITY MANAGEMENT PROCESS

3.1. GENERAL.

The DoD vulnerability management process is the cyclical practice of five steps to identify, classify, remediate, and mitigate vulnerabilities. These steps are Vulnerability Identification, Vulnerability Analysis, Analysis Reporting, Remediation and Mitigation, and Verification and Monitoring (see Figure 1).

Figure 1. Vulnerability Management Process



3.2. STEP 1: VULNERABILITY IDENTIFICATION.

Vulnerability identification employs security automation capabilities to identify possible vulnerabilities in organizational assets. These capabilities, combined with security control methodologies, provide additional means to identify vulnerabilities. There are six prime methods for vulnerability identification:

a. Vulnerability Scanning.

Vulnerability scanning inspects probable areas of weakness in computers or networks. The scan identifies internal network weaknesses for missing vendor patches and scans external systems for additional vulnerabilities. The DoD Components will:

(1) Perform vulnerability scanning procedures using the guidelines in NIST SP 800-115 as reference.

(2) Use the Common Vulnerability and Exposure website available at https://cve.mitre.org/about/index.html#why_cve to identify publicly known cybersecurity vulnerabilities

(3) Identify software requiring patches or updates.

(4) Identify unpatched vulnerabilities using automated services wherever possible and use manual processes only when necessary.

(5) Identify and maintain oversight of acquired, created, and discovered software; track software deployed on systems, subsystems, and system components.

(6) Implement scanning programs to identify gaps and deficiencies in the function and coverage of automated patching systems.

b. Penetration Testing.

Penetration testing simulates an attack on a computer or network to find vulnerabilities. The DoD Components will:

(1) Perform penetration testing considering cost and time available.

(2) Perform penetration testing using the guidelines in NIST SP 800-115 as reference.

c. Security Controls Assessment.

Security controls assessment tests the security controls of systems, subsystems, or system components to ensure the controls correctly identify and detect vulnerabilities. DoD procedures for security control assessment are located on the DoD Risk Management Framework Knowledge Service available at https://rmfks.osd.mil/rmf/RMFImplementation/AssessControls/Pages/DevelopPlan.aspx

d. Historical Documentation.

The DoD Components will cross-reference previous incident reports and logs with the Common Vulnerability and Exposure System, risk assessment data, and vendor bulletins to identify vulnerabilities.

e. Coordinated VDP

The DoD VDP maintains a coordinated vulnerability disclosure method. Locate the purpose, overview, scope, reporting procedures, and guidelines for the program at https://hackerone.com/deptofdefense.

(1) Ethical hackers must comply with all applicable federal, state, and local laws in connection with their security research activities to participate in the DoD VDP.

(2) Information submitted to DoD through the VDP must be used for defensive purposes to mitigate or remediate vulnerabilities in DODIN systems, subsystems, or system components.

(3) During the VDP coordination process, the DoD Components will:

(a) Assess the severity of validated VDP vulnerabilities.

(b) Execute mitigation or remediation efforts. The system owner's remediation team and the Cyber Service Component:

1. Execute the USCYBERCOM/ JFHQ-DODIN directive or orders.

2. Validate the vulnerability.

3. Develop, implement, and execute remediation or mitigation plans.

4. Contact the DoD Component chain of command (USCYBERCOM or Chief Information Officer) to request additional information from DC3 through USCYBERCOM as required.

5. Keep the system owner informed of actions throughout the process and completion of remediation and mitigation of the vulnerability.

(c) Advise their authorizing officials of remediation and mitigation actions.

(d) Report process through their chains of command to DC3 and USCYBERCOM within VRMN

f. VEP

The VEP is used by the USG to balance whether to disseminate vulnerability information to the vendor/supplier in the expectation that it will be patched, or to temporarily restrict the knowledge of the vulnerability to the USG, and potentially other partners, so that it can be used for national security and law enforcement purposes, such as intelligence collection, military operations, and/or counterintelligence.

(1) DoD Components will, except NSA, use existing vulnerability management processes to identify and submit vulnerabilities to USCYBERCOM for review and submission to the VEP in coordination with USD(P) or the CJCS, as applicable.

(2) NSA will submit vulnerabilities directly to the VEP.

3.3. STEP 2: VULNERABILITY ANALYSIS.

Vulnerability analysis evaluates vulnerabilities through impact assessment and analysis prioritization to assign severity levels to vulnerabilities as quickly as possible.

a. Impact Assessment.

An impact assessment determines the primary historical, recent, and probable impacts connected with the vulnerability and analyzes the underlying cause of those impacts. The DoD Components will perform impact assessments to determine the likely expected loss of integrity, confidentiality, and availability if the vulnerability is not remediated or mitigated.

b. Analysis Prioritization.

Analysis prioritization manages the prioritization and urgency of different vulnerabilities to address highly critical requirements immediately. Impact assessment results, environmental metrics, base metrics, and temporal metrics determine prioritization through the Common Vulnerability Scoring System (CVSS). DoD Components will prioritize vulnerabilities to address the most critical vulnerabilities first.

(1) The CVSS provides a uniform and standardized vulnerability scoring method, an open framework, and an ability to prioritize risk to analyze identified vulnerabilities against different metrics (e.g., base metrics, temporal metrics, and environmental metrics). NIST Interagency Report 7435 contains detailed guidelines for the use of the CVSS and its applicability to federal systems.

(2) CVSS calculators compute base, temporal, or environmental scores. The CVSSv3.1 calculator is available at https://www.first.org/cvss/calculator/3.1

(3) The NIST National Vulnerability Database is a registry of all known reported vulnerabilities, which maintain a bulletin web site that includes CVSS base scores. NIST provides these web-based bulletins in addition to XML and RSS feeds free for use. The registry is available at http://nvd.nist.gov/nvd.cfm and http://nvd.nist.gov/download.cfm#XML.

3.4. STEP 3: ANALYSIS REPORTING.

a. The DoD Components will draft an analysis report to display the output of the vulnerability analysis. The analysis report must include one or more of the following:

(1) Name of the vulnerability.

(2) Date of discovery.

(3) Recommendation to correct the vulnerability.

(4) The CVSS score.

(5) The CVSS severity rating.

(6) Details of how the loss of confidentiality, integrity, or availability could affect DoD operations, organizational assets, or individuals (e.g., limited, serious, catastrophic, or cataclysmic effects).

b. When generating the analysis report, the DoD Components will:

(1) Report all vulnerabilities immediately upon discovery.

(2) Use the CVSS 3.1 Qualitative Severity Rating scheme listed in Table 1.

(a) Any vulnerability with a minimum CVSS score of 0.1 and 3.9 has a severity rating of (Low); there is a limited adverse effect on DoD organizational operations, organizational assets, or individuals.

(b) Any vulnerability with a minimum CVSS score of 4.0 and 6.9 has a severity rating of (Medium); there is a serious adverse effect on DoD organizational operations, organizational assets, or individuals.

(c) Any vulnerability with a minimum CVSS score of 7.0 and 8.9 has a severity rating of (High); there is a catastrophic adverse effect on DoD organizational operations, organizational assets, or individuals.

(d) Any vulnerability with a minimum CVSS score of 9.0 and 10.0 has a severity rating of (Critical); there is a cataclysmic adverse effect on DoD organizational operations, organizational assets, or individuals.

Table 1. CVSS Qualitative Severity Rating Scale

CVSS Score	Severity Rating
0.0	**None**
0.1-3.9	**Low**
4.0-6.9	**Medium**
7.0-8.9	**High**
9.0-10.0	**Critical**

3.5. STEP 4: REMEDIATION AND MITIGATION.

Remediation occurs when the vulnerability is eliminated or removed. Mitigation occurs when the impact of the vulnerability is decreased without reducing or eliminating the vulnerability. To assess remediation and mitigation techniques, the DoD Components will:

a. Determine, on a case-by-case basis, which remediation or mitigation method is most beneficial and consider the loss of confidentiality, integrity, and availability.

b. Consider asset value, exposure factor, single loss expectancy, the annual rate of occurrence, annualized loss expectancy, and the total cost of ownership in mitigation or remediation method calculations.

c. Compute and maintain metrics (mean time to patch, average patch deployment success rate, average vulnerability exposure, and others over time), to evaluate the effectiveness of patching processes.

d. Monitor compliance, remediation, mitigation, and document deviations from established configuration procedures and settings.

e. Use standardized change management processes to implement and track configuration changes, patches, and updates to system software, firmware, and hardware.

f. Recommend configuration changes to ensure the correct application of remediation or mitigation actions.

g. Use a vulnerability scan to identify physical or virtual devices that require remediation or mitigation and correct identified gaps in automated patching systems.

h. Ensure patches are available to operators of patch deployment systems for software, firmware, and hardware not supported by enterprise systems.

i. Establish infrastructure discovery and procedures to gain logical or physical control of non-compliant devices and bring them into compliance in accordance with respective device compliance policies.

j. Destroy devices or media in accordance with CNSSI 4004.1.

k. Implement secure configurations for software, firmware, and hardware in accordance with applicable DoD security technical implementation guides, NSA/CSS security implementation and mitigation guidance, and NIST mitigation guidelines.

3.6. STEP 5: VERIFICATION AND MONITORING.

DoD Components will verify the remediation or mitigation method implemented on identified vulnerabilities and perform the continuous monitoring required to limit further exploitation. This verification includes actions to:

a. Verify the efficiency of the remediation or mitigation method upon completion of implementation, which provides for re-establishing the baseline configuration.

b. Compare successive vulnerability scans to ensure that the vulnerability is remediated or mitigated.

c. Monitor remediated or mitigated systems, subsystems, or system components for any more codependent vulnerabilities.

d. Conduct monthly non-authenticated and authenticated vulnerability scans to obtain accurate system information for continuous monitoring of previously affected systems.

e. Store logs in a central repository or security information and event management platform.

f. Comply with the DoD Information Security Continuous Monitoring program to meet Federal Information Security Modernization Act continuous monitoring requirements.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
CHCSS	Chief, Central Security Service
CJCS	Chairman of the Joint Chiefs of Staff
CNSSI	Committee on National Security Systems Instruction
CSS	Central Security Service
CVSS	Common Vulnerability Scoring System
DC3	DoD Cyber Crime Center
DIRNSA	Director, National Security Agency
DISA	Defense Information Systems Agency
DoDI	DoD instruction
DODIN	DoD Information Network
DoD SISO	DoD Senior Information Security Officer
ERB	Equities Review Board
ES	Executive Secretariat
JFHQ-DODIN	Joint Force Headquarters-DoD Information Network
NIST	National Institute of Standards and Technology
NSA	National Security Agency
SME	subject matter expert
US-CERT	U.S. Computer Emergency Readiness Team
USCYBERCOM	United States Cyber Command
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USD(P)	Under Secretary of Defense for Policy
USG	U.S. Government
VDP	Vulnerability Disclosure Program
VEP	Vulnerabilities Equities Process
VRMN	Vulnerability Report Management Network

G.2. DEFINITIONS.

Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

TERM	DEFINITION
active response	Sequence of actions performed specifically to mitigate a detected threat.
automated patch management	Ability to retrieve and distribute system software and configuration patches, updates, and fixes in a machine-to-machine manner to reduce the amount of human intervention and expedite the patch management process.
base metrics	The measurement of qualities intrinsic to a vulnerability.
cataclysmic	Above and beyond catastrophic. Causing an extensive amount of destruction, or a sudden, violent change.
catastrophic	Causing a large amount of destruction, or a violent change.
coordinated vulnerability disclosure	A method of disclosure that involves a set of activities, including recognizing and involving partners, mediating, communicating, and other planning to facilitate vulnerability disclosure.
cybersecurity	Defined in CNSSI 4009.
device	A unit of physical equipment or hardware that gives at least one figuring capacities inside a computer operating system.
directive authority for cyberspace operations	Defined in DoD Dictionary of Military and Associated Terms.
environmental metrics	Measurement for vulnerabilities that depend on a particular implementation or environment.
firmware	Defined in CNSSI 4009.
mitigation	Act of reducing risk by taking some other action generally outside the domain of the influenced system, which cannot be remediated.
newly discovered vulnerability	A zero-day vulnerability or new zero-day vulnerability information.
patch management	Defined in CNSSI 4009.

TERM	DEFINITION
publicly known vulnerability	A vulnerability is publicly known if the vendor is aware of its existence, and vulnerability information can be found in the public domain (e.g., published documentation, Internet, trade journals).
remediation	Actions taken to eliminate an identified risk.
risk acceptance	Defined in NIST SP 800-30.
software	Defined in CNSSI 4009.
system	Defined in CNSSI 4009.
system component	Defined in NIST Special Publication 800-37.
temporal metrics	Measurement of characteristics that evolve over the lifetime of vulnerability.
unique item identifiers	Defined in DoDI 8320.04.
virtual device	A device file that has no associated hardware.
vulnerability	Defined in CNSSI 4009.
vulnerability management	The practice of identification, classification, remediation, and mitigation of vulnerabilities in systems, subsystems, and system components.
zero-day vulnerability	Previously unknown hardware, firmware, or software vulnerability.

REFERENCES

Committee on National Security Systems Instruction No. 1253, "Security Categorization and Control Selection for National Security Systems," March 27, 2014

Committee on National Security Systems Instruction No. 4004.1, "Destruction and Emergency Protection Procedures for COMSEC and Classified Material," January 10, 2008

Committee on National Security Systems Instruction No. 4009, "Committee on National Security Systems (CNSS) Glossary," April 6, 2015, as amended

DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014, as amended

DoD Directive 5505.13E, "DoD Executive Agent (EA) for the DoD Cyber Crime Center (DC3)," March 1, 2010, as amended

DoD Instruction 5000.02T, "Operation of the Defense Acquisition System," January 23, 2020

DoD Instruction 6530.01, "Defense Medical Logistics Program," August 23, 2017

DoD Instruction 8310.01, "Information Technology Standards in the DoD," July 31, 2017, as amended

DoD Instruction 8320.03, "Unique Identification (UID) Standards for Supporting the DoD Information Enterprise," November 4, 2015, as amended

DoD Instruction 8320.04, "Item Unique Identification (IUID) Standards for Tangible Personal Property," September 3, 2015, as amended

DoD Instruction 8500.01, "Cybersecurity," March 4, 2014, as amended

Food and Drug Administration, FDA-2015-D-5105, "Postmarket Management of Cybersecurity in Medical Devices," December 2016

Food and Drug Administration, FDA-2013-S-0610, "Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software," January 2005

National Institute of Standards and Technology Interagency Report 7435, "The Common Vulnerability Scoring System (CVSS) and Its Applicability to Federal Agency Systems," August 2007

National Institute of Standards and Technology Special Publication 800-30, "Revision 1, "Guide for Conducting Risk Assessments," September 2012

National Institute of Standards and Technology Special Publication 800-37, "Revision 2, "Risk Management Framework for Information Systems and Organizations," December 2018

National Institute of Standards and Technology Special Publication 800-115, "Technical Guide to Information Security Testing and Assessment," December 2018

Office of the Chairman of the Joint Chiefs of Staff, "DoD Dictionary of Military and Associated Terms," current edition

The White House, Office of the Press Secretary, "Vulnerabilities Equities Policy and Process for the United States Government," November 15, 2017

United States Code, Title 44