Information Technology (IT) Risk Assessment (RA) Standard

January 18, 2024

U.S. Department of Education (ED)

Office of the Chief Information Officer (OCIO)

Information Assurance Services (IAS)

Questions about the policies outlined in this document should be directed to Information Assurance Services (IAS) at **IAS_Governance@ed.gov**

APPROVAL

STEVEN HERNANDEZ

Digitally signed by STEVEN HERNANDEZ
Date: 2024.01.18 18:59:09 -05'00'

Steven Hernandez
Director, IAS/Chief Information Security Officer (CISO)

Revision History

The table below identifies all changes that have been incorporated into this document.

Version	Date	Summary of Changes
1.0	12/22/2021	Initial draft of new standard which combines National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5 controls, including ED specific control parameter values, with existing policy standards.
1.1	1/14/2022	Update to incorporate feedback from Information Assurance Services (IAS), Governance, Risk and Policy (GRP) Team.
1.2	1/31/2022	Update to incorporate feedback from IAS; address new security measures required by Executive Order (EO) 14028, including Office of Management and Budget (OMB) regulations and memoranda and updated NIST guidance issued to comply with the EO.
1.3	1/31/2023	Annual review. Correct broken links and add link to HVA control overlays. Update Overlay RA-2 ED-03; add Overlays RA-2 ED-05 and RA-2 ED-06.
5.4	1/18/2024	Aligned document major version number to align with NIST SP 800-53 revision number. Clean up formatting and numbering throughout and update broken links. Section 2, Standards was updated to include the description of incorporating organizationally defined parameters (ODP) for controls that may be necessary from external control overlays (e.g., High Value Assets [HVA]). Inserted references to NIST SP 800-53B tailoring guidance. Updated Section 4, Acronyms as appropriate. Updated language in controls RA-01, RA-02 ED-03, RA-02 ED-04, RA-02 ED-05, RA-02 ED-06, and RA-03. Added controls RA-05(03), RA-05(06), RA-05(08), and RA-05(10). Added "leading zeros" to control identifiers in alignment with patch release of NIST SP 800-53 (Release 5.1.1) to applicable controls, enhancements, and overlays.

Table of Contents

1 INTRODUCTION

This governance document establishes U.S. Department of Education (ED or Department) information technology (IT) system risk assessment controls standards necessary to improve the efficiency of operation or security of Department information systems and comply with Federal laws, regulations, Executive Orders (EO), Emergency Orders, Binding Operational Directives (BOD), and Department Administrative Communications System Directives (ACSD) and Handbooks. In doing so, these standards supersede any prior governance documentation establishing such standards.

1.1 Purpose

The Federal Information Security Modernization Act (FISMA)[1] and implementing governance Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*[2], requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, and services that are either fully or partially provided, including agency-hosted, outsourced, and cloud-based solutions. Federal Information Processing Standards (FIPS) Publication (PUB) 200, *Minimum Security Requirements for Federal Information and Information Systems*[3], mandates the use of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations*[4], as amended, as baseline information system controls.

1.2 Scope

These standards apply to all information and information systems that support the operations and assets of the Department, including those provided or managed by another agency, contractor, or other source, as well as services that are either fully or partially provided, including Department-hosted, outsourced, and cloud-based solutions. Principal Offices, employees, contractors, external service providers and system users are required to comply with these risk assessment control standards.

[1] Public Law 113-283-Dec. 18, 2014, https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf

[2] Office of Management and Budget (OMB) Circular A-130, https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf

[3] FIPS 200, https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.200.pdf

[4] NIST SP 800-53, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

2 STANDARDS

The Department standards for IT system risk assessment controls are organized to follow the order in which controls are presented in the current version of NIST SP 800-53. To define a control baseline for Department information systems, a FIPS PUB 199 categorization level (e.g., Low [L], Moderate [M] and High [H]) is assigned to each requirement. This designator indicates a requirement applies to information systems categorized at that FIPS PUB 199 impact-level. Designators are also used to indicate when NIST SP 800-53 Privacy (P) baseline controls are required. To manage risk to within the Department's risk tolerance and appetite, control overlays are provided when the Department requires implementation of control(s) that are not required by the FIPS PUB 199 impact-level or privacy baseline.

In addition to the controls required by this standard, High Value Assets (HVAs) must implement and comply with the current version of the HVA Control Overlay[5] issued and maintained by the U.S. Department of Homeland Security (DHS), Cybersecurity & Infrastructure Security Agency (CISA). Systems that process federal tax return information (FTI) must implement and comply with the Internal Revenue Service (IRS) Publication 1075[6], *Tax Information Security Guidelines for Federal, State and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information.* Systems that are Federal Risk and Authorization Management Program (FedRAMP) authorized must implement and comply with the FedRAMP identified baselines[7].

Throughout the standard, there are controls captured that have not been scoped to any specific security or privacy baseline. This is intentional as all controls for identified external overlays and baselines (e.g., FedRAMP, IRS, HVA), that may apply to systems within the Department, have been incorporated into the standard. This ensures the organization defined parameters (ODPs) for controls within the Department have been clearly defined in a consistent manner.

This standard directly supports the Department's integration of the NIST Cybersecurity Framework (CSF) and Privacy Framework (PF) in focusing on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the Department's risk management processes. Refer to APPENDIX A - BASELINE CONTROL PARAMETER SUMMARY for a summary of controls by baseline and corresponding NIST CSF and NIST PF categories and subcategories.

[5] https://www.cisa.gov/publication/high-value-asset-control-overlay

[6] IRS Publication 1075 https://www.irs.gov/pub/irs-pdf/p1075.pdf

[7] FedRAMP baselines https://www.fedramp.gov/baselines/

2.1 RA-01 Risk Assessment Policy and Procedures (P, L, M, H)

The Department shall develop, document, and disseminate to all ED employees, contractors, and users authorized to access to ED information systems, or systems operated or maintained on behalf of ED, or ED information as defined in ACSD-OCIO-004[8], *Cybersecurity Policy* a Department-level IT system risk assessment policy (e.g., this document) that:

(a) addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;

(b) is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

(c) authorizes the Department Chief Information Security Officer (CISO) and Department Chief Information Officer (CIO) to issue subordinate standards, procedures, and memos, with the same authority and enforcement as ACSD-OCIO-004, Cybersecurity Policy.

The Department CISO in conjunction with the Senior Agency Official for Privacy (SAOP) are designated to manage the development, documentation, and dissemination of the Department-level IT system risk assessment policy.

This policy shall be reviewed and updated annually (i.e., each fiscal year) and following the identification of evolving threats; issuance of new or significantly changed existing Federal laws, executive orders, directives, regulations, and ED policies; identification of emerging technology and information technology service delivery models; and determination that adjustments are deemed necessary to improve its effectiveness based upon feedback from Principal Office personnel.

Principal Office (PO) Information System Owners (ISO) and Information System Security Officers (ISSOs) are required to manage the development, documentation, and dissemination of system specific procedures to facilitate the implementation of this policy standard and associated risk assessment controls. The ISO and ISSO shall review IT system risk assessment procedures annually (i.e., each fiscal year) and following the identification of evolving threats; issuance of new or significantly changed existing Federal laws, executive orders, directives, regulations, and ED policies; identification of emerging technology and information technology service delivery models; and determination that adjustments are deemed necessary to improve its effectiveness based upon feedback from Principal Office personnel.

[8] Also known as OCIO: 3-112.

2.2 RA-02 Security Categorization (L, M, H and Control Overlay)

a. Categorize the system and information it processes, stores, and transmits;

b. Document the security categorization results, including supporting rationale, in the security plan for the system; and

c. Verify that the Authorizing Official (AO), or AO Designated Representative, and the Senior Agency Official for Privacy reviews and approves the security categorization decision."

Control Overlay RA-2 ED-01 (L, M, H): Affirm through the issuance of this standard that the Department's Cyber Security Assessment and Management (CSAM) tool is the authoritative source for developing, managing and maintaining the information technology (IT) systems; the system of record for FISMA reporting; and the enterprise tool used to support Cybersecurity Risk Management Framework (CRMF) processes.

Control Overlay RA-02 ED-02 (L, M, H): Use CSAM tool functionality to:

a. Document information types and conduct the security categorization of information systems in accordance with the current, finalized version of FIPS Publications 199 and NIST SP 800-60, as amended. Note: "Other" is not a valid business area or information type.

b. Review and maintain information types as required to maintain the accuracy of the information types and security categorization of systems throughout the system lifecycle.

Control Overlay RA-02 ED-03 (L, M, H): Assign a minimum impact level of "Moderate" for the confidentiality security objective for systems involving Personally Identifiable Information (PII) unless the Chief Privacy Officer/Senior Agency Official for Privacy has reviewed and determined that a low categorization would be appropriate. Elevate the confidentiality security objective to "High" if warranted by a risk-based assessment.

Control Overlay RA-02 ED-04 (L, M, H): Assign a minimum impact level of "Moderate" for confidentiality, integrity, and availability for all Chief Financial Officer (CFO) Designated Systems. Elevate the integrity objective to "High" if warranted by a risk-based assessment.

Control Overlay RA-02 ED-05 (L, M, H): Assign a minimum impact level of "Moderate" or "High" for confidentiality impact for all systems which are included in a Principal Office Business Continuity Plan or that support a Mission Essential Function (MEF) defined in the Department Continuity of Operations Plan (COOP).

Control Overlay RA-02 ED-06 (L, M, H): Apply the Business Impact Analysis (BIA) output to develop asset categorization, impact values, and requirements for the protection of critical or sensitive assets, enable effective risk management and the subsequent integration of reporting and monitoring at the enterprise level, and support integration of Enterprise Risk Management (ERM) with Cybersecurity Risk Management, as described in the NIST Interagency Report (IR) 82866 series.

2.3 RA-03 Risk Assessment (P, L, M, H and Control Overlay)

a. Conduct a risk assessment, including:

   1. Identifying threats to and vulnerabilities in the system;
   2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and
   3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;

b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;

c. Document risk assessment results in the Security Assessment Report (SAR), Privacy Impact Assessment (PIA), when a PIA is required, and the Facility Risk Assessment Report, which is required when a system is deployed in a traditional, non-cloud-based datacenter or hosting environment;

d. Review risk assessment results annually or whenever an update to the risk assessment is made;

e. Disseminate risk assessment results to the AO, CISO, SAOP, ISO, and ISSO; and

f. Update the risk assessment in accordance with the frequency defined in Department policy for each risk result documentation type or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.

Control Overlay RA-03 ED-01 (L, M, H): Use the ED CSF Risk Scorecard to:

   a. Define risk profiles which align and prioritize cybersecurity activities with business/mission requirements, risk tolerance/appetite, and resources.

   b. Perform regular NIST CSF-based risk assessments of FISMA-reportable systems, including HVAs, to identify gaps, improvement opportunities and support enhancements to incident response capabilities.

   c. Enable the AO, ISO, and ISSO to view, understand, and manage cybersecurity risk to their assigned systems.

   d. Inform cybersecurity strategic planning activities.

2.3.1 RA-03(01) Risk Assessment | Supply Chain Risk Assessment (L, M, H)

a. Assess supply chain risks associated with ED systems, components, and services as defined in the ED Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Roadmap and Plan.

b. Update the supply chain risk assessment annually or as defined in the ED ICT SCRM Roadmap and Plan or the Department's Supply Chain Risk Management standard, when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.

2.4 RA-05 Vulnerability Monitoring and Scanning (L, M, H)

a. Monitor and scan for vulnerabilities in the system and hosted applications in accordance with *APPENDIX B - VULNERABILITY SCAN FREQUENCY AND REMEDIATION REQUIREMENTS* and when new vulnerabilities potentially affecting the system are identified and reported;

b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

    1. Enumerating platforms, software flaws, and improper configurations;

    2. Formatting checklists and test procedures; and

    3. Measuring vulnerability impact;

c. Analyze vulnerability scan reports and results from vulnerability monitoring;

d. Remediate legitimate vulnerabilities in as required to comply with the response times defined in *APPENDIX B - VULNERABILITY SCAN FREQUENCY AND REMEDIATION REQUIREMENTS* and in accordance with an organizational assessment of risk;

e. Share information obtained from the vulnerability monitoring process and control assessments with ISO, ISSOs, and other relevant system stakeholders to help eliminate similar vulnerabilities in other systems; and

f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

2.4.1 RA-05(02) Vulnerability Monitoring and Scanning | Update Vulnerabilities to be Scanned (L, M, H)

Update the system vulnerabilities to be scanned no more than 24 hours prior to conducting a scan and in accordance with each tool's vendor data definition releases.

2.4.2 RA-05(03) Vulnerability Monitoring and Scanning | Breadth and Depth of Coverage

Define the breadth and depth of vulnerability scanning coverage.

2.4.3 RA-05(04) Vulnerability Monitoring and Scanning | Discoverable Information (H)

Determine information about the system that is discoverable and take the following actions:

a. Notify the ISO and ISSO, move or obfuscate the discoverable information or take other actions, as appropriate.

b. Share the discoverable information with the ED Security Operations Center (EDSOC) within one (1) hour of identification if it is determined that knowledge of the discoverable information could be detrimental to a system's security posture.

2.4.4 RA-05(05) Vulnerability Monitoring and Scanning | Privileged Access (M, H)

Implement privileged access authorization to all information system components as applicable (e.g., operating system, database, web application, containers, etc.) for all vulnerability scanning activities.

2.4.5 RA-05(06) Vulnerability Monitoring and Scanning | Automated Trend Analysis

Compare the results of multiple vulnerability scans using the implemented automated scanning capability.

2.4.6 RA-05(08) Vulnerability Monitoring and Scanning | Review Historic Audit Logs

Review historic audit logs to determine if a vulnerability identified in a defined critical component has been previously exploited within the log retention period for the component with the identified vulnerability.

2.4.7 RA-05(10) Vulnerability Monitoring and Scanning | Correlate Scanning Information

Correlate the output from vulnerability scanning tools to determine the presence of multi-vulnerability and multi-hop attack vectors.

2.4.8 RA-05(11) Vulnerability Monitoring and Scanning | Public Disclosure Program (L, M, H and Control Overlay)

Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.

Control Overlay RA-05(11) ED-01 (L, M, H): Develop, publish, and maintain a Vulnerability Disclosure Policy which complies with Department of Homeland Security, Binding Operational Directive 20-01.

2.5 RA-07 Risk Response (P, L, M, H)

Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.

2.6 RA-08 Privacy Impact Assessments (P)

Conduct Privacy Impact Assessments for systems, programs, or other activities before:

a. Developing or procuring information technology that processes personally identifiable information; and

b. Initiating a new collection of personally identifiable information that:

   1. Will be processed using information technology.

   2. Includes personally identifiable information permitting the physical or virtual (online) contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, ten or more individuals, other than agencies, instrumentalities, or employees of the federal government.

2.7 RA-09 Criticality Analysis (M, H)

Identify critical system components and functions by performing a criticality analysis for all FISMA reportable systems and critical system components initially at the system design/architectural design phase of the Enterprise Program Management Review Framework (EPMR) and continuously through the entire lifecycle, including operations and maintenance (O&M) phase if there are significant system changes impacting criticality of system components.

3 RISK ACCEPTANCE/POLICY EXCEPTIONS

Deviations from the Department policies, Instructions, Standards, Procedures or Memos must be approved and documented through the Department's Risk Acceptance process. Deviations that introduce additional risks to the enterprise must be submitted through the Department Risk Acceptance Form (RAF) and must be approved by the ED CISO (as delegated). Requests must justify the reason for the deviation(s)/exception(s) as well as the compensating security controls implemented to secure the device or information, if applicable. Policy deviations that do not introduce additional risks do not need to be submitted through the Department RAF but will need to be approved by the Department CISO (as delegated).

4 ACRONYMS

Acronym	Definition
ACSD	Administrative Communications System Directives
AO	Authorizing Official
BIA	Business Impact Analysis
BOD	Binding Operational Directive
CDM	Continuous Diagnostics and Mitigation
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISA	Cybersecurity & Infrastructure Security Agency
CISO	Chief Information Security Officer
CM.PO-P	Communication Policies, Processes, and Procedures
CM-P	Communicate-P
COOP	Continuity of Operations Plan
CRMF	Cybersecurity Risk Management Framework
CSAM	Cyber Security Assessment and Management
CSF	Cybersecurity Framework
DE	Detect
DE.AE	Anomalies and Events
DE.CM	Security Continuous Monitoring
DE.DP	Detection Processes
Department	U.S. Department of Education
DHS	U.S. Department of Homeland Security
DNS	Domain Name System
ED	U.S. Department of Education
EDSOC	ED Security Operations Center
EO	Executive Order
EPMR	Enterprise Program Management Review
ERM	Enterprise Risk Management
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
FTRI	Federal Tax Return Information
GRP	Governance, Risk and Policy
GV.MT-P	Monitoring and Review
GV.PO-P	Governance Policies, Processes, and Procedures
GV-P	Govern-P
H	High
HVA	High Value Asset
IAS	Information Assurance Services
ICT	Information and Communications Technology
ID	Identify
ID.AM	Asset Management
ID.BE	Business Environment
ID.BE-P	Business Environment
ID.DE-P	Data Processing Ecosystem Risk Management

Acronym	Definition
ID.GV	Governance
ID.RA	Risk Assessment
ID.RA-P	Risk Assessment
ID.RM	Risk Management Strategy
ID.SC	Supply Chain Risk Management
ID-P	Identify-P
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IR	Interagency Report
IRS	Internal Revenue Service
ISO	Information System Owner
ISP	Internet Service Provider
ISSO	Information System Security Officer
IT	Information Technology
L	Low
M	Moderate
MEF	Mission Essential Function
NIST	National Institute of Standards and Technology
O&M	Operations and Maintenance
OCIO	Office of the Chief Information Officer
ODP	Organizationally Defined Parameters
OMB	Office of Management and Budget
P	Privacy
PF	Privacy Framework
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PO	Principal Office
PR	Protect
PR.PO-P	Data Protection Policies, Processes, and Procedures
PR-P	Protect-P
PUB	Publication
RA	Risk Assessment Family
RAF	Risk Acceptance Form
RS	Respond
RS.AN	Analysis
RS.MI	Mitigation
SAOP	Senior Agency Official for Privacy
SAR	Security Assessment Report
SCRM	Supply Chain Risk Management
SP	Special Publication

APPENDIX A - BASELINE CONTROL PARAMETER SUMMARY

The applicability for each baseline control parameter is shown below.

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
RA-01	Policy and Procedures	X	X	X	X	ID.GV, PR.IP, RS.AN, DE.DP, GV.PO-P, GV.MT-P, PR.PO-P	ID.GV-4, PR.IP-12, RS.AN-5, DE.DP-2, GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6, GV.PO-P6, PR.PO-P10
RA-02	Security Categorization		X	X	X	ID.AM, ID.GV, ID.RA, ID.RA-P	ID.AM-5, ID.GV-4, ID.RA-4, ID.RA-5, ID.RA-P4
RA-02(01)	Security Categorization | Impact-level Prioritization					ID.AM, ID.GV, ID.RA, ID.RA-P	ID.AM-5, ID.GV-4, ID.RA-4, ID.RA-5, ID.RA-P4
RA-03	Risk Assessment	X	X	X	X	ID.GV, ID.RA, ID.SC, PR.IP, DE.AE, RS.AN, RS.MI, ID.RA-P, ID.DE-P, GV.PO-P, GV.MT-P, PR.PO-P	ID.GV-4, ID.RA-1, ID.RA-3, ID.RA-4, ID.RA-5, ID.SC-2, PR.IP-12, DE.AE-4, RS.AN-2, RS.AN-4, RS.MI-3, ID.RA-P1, ID.RA-P3, ID.RA-P4, ID.DE-P2, GV.PO-P6, GV.MT-P1, GV.MT-P5, PR.PO-P10

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
RA-03(01)	Risk Assessment | Supply Chain Risk Assessment		X	X	X	ID.GV, ID.RA, ID.SC, PR.IP, DE.AE, RS.AN, RS.MI, ID.RA-P, ID.DE-P, GV.PO-P, GV.MT-P, PR.PO-P	ID.GV-4, ID.RA-1, ID.RA-3, ID.RA-4, ID.RA-5, ID.SC-2, PR.IP-12, DE.AE-4, RS.AN-2, RS.AN-4, RS.MI-3, ID.RA-P1, ID.RA-P3, ID.RA-P4, ID.DE-P2, GV.PO-P6, GV.MT-P1, GV.MT-P5, PR.PO-P10
RA-03(02)	Risk Assessment | Use of All-source Intelligence					ID.GV, ID.RA, ID.SC, PR.IP, DE.AE, RS.AN, RS.MI, ID.RA-P, ID.DE-P, GV.PO-P, GV.MT-P, PR.PO-P	ID.GV-4, ID.RA-1, ID.RA-3, ID.RA-4, ID.RA-5, ID.SC-2, PR.IP-12, DE.AE-4, RS.AN-2, RS.AN-4, RS.MI-3, ID.RA-P1, ID.RA-P3, ID.RA-P4, ID.DE-P2, GV.PO-P6, GV.MT-P1, GV.MT-P5, PR.PO-P10

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
RA-03(03)	Risk Assessment | Dynamic Threat Awareness					ID.GV, ID.RA, ID.SC, PR.IP, DE.AE, RS.AN, RS.MI, ID.RA-P, ID.DE-P, GV.PO-P, GV.MT-P, PR.PO-P	ID.GV-4, ID.RA-1, ID.RA-3, ID.RA-4, ID.RA-5, ID.SC-2, PR.IP-12, DE.AE-4, RS.AN-2, RS.AN-4, RS.MI-3, ID.RA-P1, ID.RA-P3, ID.RA-P4, ID.DE-P2, GV.PO-P6, GV.MT-P1, GV.MT-P5, PR.PO-P10
RA-03(04)	Risk Assessment | Predictive Cyber Analytics					ID.GV, ID.RA, ID.SC, PR.IP, DE.AE, RS.AN, RS.MI, ID.RA-P, ID.DE-P, GV.PO-P, GV.MT-P, PR.PO-P	ID.GV-4, ID.RA-1, ID.RA-3, ID.RA-4, ID.RA-5, ID.SC-2, PR.IP-12, DE.AE-4, RS.AN-2, RS.AN-4, RS.MI-3, ID.RA-P1, ID.RA-P3, ID.RA-P4, ID.DE-P2, GV.PO-P6, GV.MT-P1, GV.MT-P5, PR.PO-P10
RA-05	Vulnerability Monitoring and Scanning		X	X	X	ID.RA, PR.IP, DE.AE, DE.CM, DE.DP, RS.AN,	ID.RA-1, PR.IP-12, DE.AE-2, DE.CM-8, DE.DP-4, DE.DP-5,

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
						RS.MI, PR.PO-P	RS.AN-1, RS.MI-3, PR.PO-P10
RA-05(02)	Vulnerability Monitoring and Scanning | Update Vulnerabilities to Be Scanned		X	X	X	ID.RA, PR.IP, DE.AE, DE.CM, DE.DP, RS.AN, RS.MI, PR.PO-P	ID.RA-1, PR.IP-12, DE.AE-2, DE.CM-8, DE.DP-4, DE.DP-5, RS.AN-1, RS.MI-3, PR.PO-P10
RA-05(03)	Vulnerability Monitoring and Scanning | Breadth and Depth of Coverage					ID.RA, PR.IP, DE.AE, DE.CM, DE.DP, RS.AN, RS.MI, PR.PO-P	ID.RA-1, PR.IP-12, DE.AE-2, DE.CM-8, DE.DP-4, DE.DP-5, RS.AN-1, RS.MI-3, PR.PO-P10
RA-05(04)	Vulnerability Monitoring and Scanning | Discoverable Information				X	ID.RA, PR.IP, DE.AE, DE.CM, DE.DP, RS.AN, RS.MI, PR.PO-P	ID.RA-1, PR.IP-12, DE.AE-2, DE.CM-8, DE.DP-4, DE.DP-5, RS.AN-1, RS.MI-3, PR.PO-P10
RA-05(05)	Vulnerability Monitoring and Scanning | Privileged Access			X	X	ID.RA, PR.IP, DE.AE, DE.CM, DE.DP, RS.AN, RS.MI, PR.PO-P	ID.RA-1, PR.IP-12, DE.AE-2, DE.CM-8, DE.DP-4, DE.DP-5, RS.AN-1, RS.MI-3, PR.PO-P10

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
RA-05(06)	Vulnerability Monitoring and Scanning | Automated Trend Analyses					ID.RA, PR.IP, DE.AE, DE.CM, DE.DP, RS.AN, RS.MI, PR.PO-P	ID.RA-1, PR.IP-12, DE.AE-2, DE.CM-8, DE.DP-4, DE.DP-5, RS.AN-1, RS.MI-3, PR.PO-P10
RA-05(08)	Vulnerability Monitoring and Scanning | Review Historic Audit Logs					ID.RA, PR.IP, DE.AE, DE.CM, DE.DP, RS.AN, RS.MI, PR.PO-P	ID.RA-1, PR.IP-12, DE.AE-2, DE.CM-8, DE.DP-4, DE.DP-5, RS.AN-1, RS.MI-3, PR.PO-P10
RA-05(10)	Vulnerability Monitoring and Scanning | Correlate Scanning Information					ID.RA, PR.IP, DE.AE, DE.CM, DE.DP, RS.AN, RS.MI, PR.PO-P	ID.RA-1, PR.IP-12, DE.AE-2, DE.CM-8, DE.DP-4, DE.DP-5, RS.AN-1, RS.MI-3, PR.PO-P10
RA-05(11)	Vulnerability Monitoring and Scanning | Public Disclosure Program		X	X	X	ID.RA, PR.IP, DE.AE, DE.CM, DE.DP, RS.AN, RS.MI, PR.PO-P	ID.RA-1, PR.IP-12, DE.AE-2, DE.CM-8, DE.DP-4, DE.DP-5, RS.AN-1, RS.MI-3, PR.PO-P10
RA-06	Technical Surveillance Countermeasures Survey						
RA-07	Risk Response	X	X	X	X	ID.RA, RS.AN, RS.MI, ID.RA-P	ID.RA-6, RS.AN-5, RS.MI-3, ID.RA-P5

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
RA-08	Privacy Impact Assessments	X				ID.RA-P, ID.DE-P, GV.PO-P, GV.MT-P, CM.PO-P	ID.RA-P1, ID.RA-P3, ID.RA-P4, ID.RA-P5, ID.DE-P2, GV.PO-P6, GV.MT-P1, GV.MT-P5, CM.PO-P1
RA-09	Criticality Analysis			X	X	ID.AM, ID.BE, ID.RA, ID.RM, ID.BE-P	ID.AM-5, ID.BE-4, ID.BE-5, ID.RA-4, ID.RM-3, ID.BE-P3
RA-10	Threat Hunting					ID.RA	ID.RA-2, ID.RA-3

APPENDIX B - VULNERABILITY SCAN FREQUENCY AND REMEDIATION REQUIREMENTS

Vulnerability scanning identifies security weaknesses within systems and allows the Department to prioritize their resources to the most critical areas. Principal Offices conduct vulnerability scans to identify and report vulnerabilities and configuration weaknesses within Department systems in accordance with requirements in the table below. The Department's Continuous Diagnostics and Mitigation (CDM) program scans all in-scope IT assets for CDM integrated information systems every 72 hours at minimum.

Scan Type	Minimum Frequency	Authentication Required?	Scope
Operating System	Weekly	Yes	Ports, protocols, services, patch levels and baseline configuration
Web Application	Monthly	Yes	
Database	Monthly	Yes	
Infrastructure components (e.g., switches, routers, guards, sensors, networked printers, scanners, and copiers)	Monthly	Yes	Ports, protocols, services and baseline configuration
DHS Cyber Hygiene (e.g., Internet-accessible systems)	As conducted by DHS		All static, public IP addresses for all internet-accessible information systems, which encompasses those systems directly managed by the Department as well as those operated on the Department's behalf. Includes any Department system that is reachable over the public internet that has a publicly routed internet protocol (IP) address or a hostname that resolves publicly in domain name system (DNS) to such an address. Does not include infrastructure that is internal to the Department's network that enables endpoints to be accessible over the internet, systems reachable from the internet but that require special configuration or access controls (e.g., via a Virtual Private Network), or shared services used by Department that are not specifically managed by the Department. Notify IAS (OCIO_IAS@ed.gov) of any changes to the Internet-facing IP inventory within three (3) days of a change; include any newly acquired public, static internet

Scan Type	Minimum Frequency	Authentication Required?	Scope
			protocol version 4 (IPv4) addresses, or any addresses recently returned to the Internet Service Provider (ISP).

Remediate legitimate vulnerabilities in accordance with the response times shown below:

Vulnerability Source	System Type	Remediation Timeframe Required
Department or Department Contractor Generated Vulnerability Scan Reports	External facing systems (including High Value Assets (HVAs) and systems or assets with FIPS PUB 199 High categorization); an external facing system, also known as an internet-accessible federal information system, is any Department system that is reachable over the public internet that has a publicly routed IP address or a hostname that resolves publicly in DNS to such an address.	• Zero-Day scan vulnerabilities must be remediated within 24-48 hours of initial detection. • Critical (Very High) scan vulnerabilities must be remediated within 15 calendar days of initial detection. • High scan vulnerabilities must be remediated within 30 calendar days of initial detection. • Moderate scan vulnerabilities must be remediated within 90 calendar days of initial detection. • Low scan vulnerabilities must be remediated within 180 calendar days of initial detection.
Department or Department Contractor Generated Vulnerability Scan Reports	Internal facing systems	• System stakeholders are allowed 30 days analysis and then the following timeline applies: - Zero-Day scan vulnerabilities must be remediated within 24-48 hours of initial detection. - Critical (Very High) scan vulnerabilities must be remediated within 15 calendar days of initial detection. - High scan vulnerabilities must be remediated within 30 calendar days of initial detection. - Moderate scan vulnerabilities must be remediated within 90 calendar days of initial detection. - Low scan vulnerabilities must be remediated within 180 calendar days of initial detection.
DHS CISA-managed catalog of known exploited vulnerabilities	All Department Systems	• Remediate each vulnerability according to the timelines set forth in the CISA-managed vulnerability catalog
DHS Cyber Hygiene Reports	All static, public IP addresses for all internet-accessible	Note: vulnerability tracking begins from the time of initial

Vulnerability Source	System Type	Remediation Timeframe Required
	information systems, which encompasses those systems directly managed by the Department as well as those operated on the Department's behalf. Includes any Department system that is reachable over the public internet that has a publicly routed IP address or a hostname that resolves publicly in DNS to such an address. Does not include infrastructure that is internal to the Department's network that enables endpoints to be accessible over the internet, systems reachable from the internet but that require special configuration or access controls (e.g., via a Virtual Private Network), or shared services used by Department that are not specifically managed by the Department.	detection, not the time when DHS provides notification to the Department. • Critical vulnerabilities must be remediated *within 15 calendar days* of initial detection. • High vulnerabilities must be remediated *within 30 calendar days* of initial detection.