Information Technology (IT) Incident Response (IR) Standard

February 9, 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: 2024.02.10 16:05:35 -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	1/14/2022	Initial draft of new standard which combines NIST SP 800-53, Revision 5 controls, including ED specific control parameter values, with existing policy standards.
1.1	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.
1.2	2/10/2023	Annual Update. Update broken links. Add footnote to HVA control reference in Section 2. Update Control Overlay IR-3 ED-01 and Control Overlay IR-8 ED-01. Updated the Standard Header. Update Section 1.2 Scope
5.3	2/9/2024	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 IR-01, IR-03 ED-01, IR-04(01). Added controls IR-03(03), IR-04(02), IR-04(06), IR-04(08), IR-04(10), IR-04(11), IR-06(02), IR-07(02), IR-09, IR-09(02), IR-09(03), and IR-09(04). 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 incident response 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 regulation 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 system incident response 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 incident response 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 issued and maintained by the Department of Homeland Security (DHS), Cybersecurity & Infrastructure Security Agency (CISA). Systems that process federal tax information (FTI) must implement and comply with the Internal Revenue Service (IRS) Publication 1075[5], *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[6].

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 NIST Privacy Framework (PF) by 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.

2.1 IR-01 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[7], *Cybersecurity Policy* a Department-level IT Incident Response policy (e.g., this document) that:

[5] IRS Publication 1075 https://www.irs.gov/pub/irs-pdf/p1075.pdf
[6] FedRAMP baselines https://www.fedramp.gov/baselines/
[7] Also known as OCIO 3-112.

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

b. is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

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 Incident Response 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 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 the Department's Incident Response policy and the associated controls. The ISO and ISSO shall review Incident Response 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.

2.2 IR-02 Incident Response Training (P, L, M, H, and Control Overlay)

a. Provide incident response training consistent with assigned roles and responsibilities:

   1. Within thirty (30) days of assuming an incident response role or responsibility or acquiring system access.

   2. When required by system changes; and

   3. Annual refresher training thereafter

b. Review and update incident response training content at least annually (i.e., each fiscal year) and following events that may precipitate an update to incident response training content including, but not limited to:

1. An incident response plan testing or response to an actual incident, to incorporate lessons learned.
2. Assessment or audit findings; or
3. Changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Control Overlay IR-02 ED-01 (L, M, H): Train all security operations personnel and incident response team members, based on their roles and responsibilities, on how to handle incidents involving Executive Order (EO)-critical software or EO-critical software platforms.

2.2.1 IR-02(01) Incident Response Training | Simulated Events (H)

Incorporate simulated events into incident response training to facilitate the required response by personnel in crisis situations.

2.2.2 IR-02(02) Incident Response Training | Automated Training Environment (H)

Provide an incident response approved training environment using ED approved interactive simulations based on real-world data.

2.2.3 IR-02(03) Incident Response Training | Breach (P)

Provide incident response training on how to identify and respond to a breach, including the organization's process for reporting a breach.

2.3 IR-03 Incident Response Testing (P, M, H, and Control Overlay)

Test the effectiveness of the incident response capability for the system at least annually (i.e., each fiscal year) using the following tests:

a. Tabletop or functional tests/checklist;
b. Strategic and tactical threat modeling;
c. Simulations;
d. Ad hoc penetration assessments; and
e. Other assessment methods identified and authorized by the Department.

Control Overlay IR-03 ED-01 (L, M, H): Use the current version of the Incident Response Plan (IRP) to document results of annual incident response plan testing. Cloud service providers (CSPs) and Shared Services are not required to upload testing artifacts into Cyber Security Assessment and Management (CSAM) but are required to document testing dates in CSAM.

2.3.1 IR-03(02) Incident Response Testing | Coordination with Related Plans (M, H)

Coordinate incident response testing with organizational elements responsible for related plans.

2.3.2 IR-03(03) Incident Response Training | Continuous Improvement

Use qualitative and quantitative data from testing to:

a. Determine the effectiveness of incident response processes;

b. Continuously improve incident response processes; and

c. Provide incident response measures and metrics that are accurate, consistent, and in a reproducible format.

2.4 IR-04 Incident Handling (P, L, M, H)

a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery.

b. Coordinate incident handling activities with contingency planning activities.

c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly.

d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

2.4.1 IR-04(01) Incident Handling | Automated Incident Handling Processes (M, H)

Support the incident handling process using ED Security Operations Center (EDSOC) automated mechanisms.

2.4.2 IR-04(02) Incident Handling | Dynamic Reconfiguration

Include the following types of dynamic reconfiguration for identified critical system components as part of the incident response capability: dynamic reconfiguration with the intent to reduce the window of time for a threat actor to maliciously exploit an incident.

2.4.3 IR-04(04) Incident Handling | Information Correlation (H)

Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.

2.4.4 IR-04(06) Incident Handling | Insider Threats

Implement an incident handling capability for incidents involving insider threats.

2.4.5 IR-04(08) Incident Handling | Correlation with External Organizations

Coordinate with interconnected external entities to correlate and share incident response requirements and reporting timelines, in accordance with United States Computer Emergency Readiness Team (US-CERT) Federal Incident Notification Guidelines, to achieve a cross-organization perspective on incident awareness and more effective incident responses.

2.4.6 IR-04(10) Incident Handling | Supply Chain Coordination

Coordinate incident handling activities involving supply chain events with other organizations involved in the supply chain.

2.4.7 IR-04(11) Incident Handling | Integrated Incident Response Team (H)

Establish and maintain an integrated incident response team that can be deployed to any location identified by the organization in 30 days or less based upon availability of staffing, funding, and tools.

2.5 IR-05 Incident Monitoring (P, L, M, H)

Track and document incidents.

2.5.1 IR-05(01) Incident Monitoring | Automated Tracking, Data Collection, and Analysis (H)

Track incidents and collect and analyze incident information using methodology within the Incident Response Plan (IRP).

2.6 IR-06 Incident Reporting (P, L, M, H, and Control Overlay)

a. Require personnel to report suspected incidents to the organizational incident response capability immediately and without unreasonable delay.

b. Report incident information to the EDSOC and ISSO.

Control Overlay IR-06 ED-01 (L, M, H): Specify timelines in accordance with the current version of NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* for public and internal incident notification timelines.

Control Overlay IR-06 ED-02 (L, M, H): Report incidents that may constitute a computer crime (violations of applicable Federal and/or State laws) to the Office of the Inspector General (OIG). *APPENDIX B – REPORTING EVENTS* provides examples of incident types which must be reported.

2.6.1 IR-06(01) Incident Reporting | Automated Reporting (M, H)

Report incidents using ED approved automated mechanisms.

2.6.2 IR-06(02) Incident Reporting | Vulnerabilities Related to Incidents

Report system vulnerabilities associated with reported incidents to identified system personnel and EDSOC.

2.6.3 IR-06(03) Incident Reporting | Supply Chain Coordination (M, H)

Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.

2.7 IR-07 Incident Response Assistance (P, L, M, H)

Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.

2.7.1 IR-07(01) Incident Response Assistance | Automation support for Availability of Information and Support (M, H)

Increase the availability of incident response information and support using ED approved automated mechanisms.

2.7.2 IR-07(02) Incident Response Assistance | Coordination with External Providers

a. Establish a direct, cooperative relationship between its incident response capability and external providers of system protection capability; and

b. Identify organizational incident response team members to the external providers.

2.8 IR-08 Incident Response Plan (IRP) (P, L, M, H, and Control Overlay)

a. Develop an incident response plan that:

1. Provides the organization with a roadmap for implementing its incident response capability; Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated;
2. Describes the structure and organization of the incident response capability;
3. Provides a high-level approach for how the incident response capability fits into the overall organization;
4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
5. Defines reportable incidents;
6. Provides metrics for measuring the incident response capability within the organization;
7. Defines the resources and management support needed to effectively maintain and mature an incident response capability;
8. Addresses the sharing of incident information;
9. Is reviewed and approved by personnel responsible for SSP approval in accordance with the Department's required authorization documentation standards; and
10. Explicitly designates responsibility for incident response to EDSOC.
    a. Distribute copies of the incident response plan to ISO, ISSO, and system personnel with incident response responsibilities;

b. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing;

c. Communicate incident response plan changes to ISO, ISSO and system personnel with incident response responsibilities; and

d. Protect the incident response plan from unauthorized disclosure and modification.

Control Overlay IR-08 ED-01 (L, M, H): Use the current version of the authorized IRP template to develop system level plans; use of these templates is not required for cloud service providers and Shared Services.

2.8.1 IR-08(01) Incident Response Plan | Breaches (P)

Include the following in the Incident Response Plan for breaches involving personally identifiable information:

a. A process to determine if notice to individuals or other organizations, including oversight organizations, is needed;

b. An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and

c. Identification of applicable privacy requirements.

2.9 IR-09 Information Spillage Response

Respond to information spills by:

a. Assigning designated incident response personnel with responsibility for responding to information spills;

b. Identifying the specific information involved in the system contamination;

c. Alerting designated incident response personnel and EDSOC of the information spill using a method of communication not associated with the spill;

d. Isolating the contaminated system or system component;

e. Eradicating the information from the contaminated system or component;

f. Identifying other systems or system components that may have been subsequently contaminated; and

g. Performing the following additional actions: reporting to all appropriate internal and external entities based on the information spilled.

2.9.1 IR-09(02) Information Spillage Response | Training

Provide information spillage response training at least annually.

2.9.2 IR-09(03) Information Spillage Response | Post-spill Operations

Implement the following procedures to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions: activation of the contingency plan.

2.9.3 IR-09(04) Information Spillage Response | Exposure to Unauthorized Personnel

Employ the following controls for personnel exposed to information not within assigned access authorizations: ensure the individuals are briefed and debriefed of the proper handling a processes for the information exposed to include governing laws, executive orders, directives, regulations, policies, standards, and guidelines regarding the restrictions imposed based on the exposure to such information.

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
BOD	Binding Operational Directive
CIO	Chief Information Officer
CISA	Cybersecurity & Infrastructure Security Agency
CISO	Chief Information Security Officer
CM.AW-P	Data Processing Awareness
CM-P	Communicate-P
CSAM	Cyber Security Assessment and Management
CSF	Cybersecurity Framework
CSP	Cloud Service Provider
DE	Detect
DE.AE	Anomalies and Events
DE.DP	Detection Processes
Department	U.S. Department of Education
DHS	U.S. Department of Homeland Security
DoS	Denial of Service
ED	U.S. Department of Education
EDSOC	ED Security Operations Center
EO	Executive Order
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
FSA	Federal Student Aid
FTRI	Federal Tax Return Information
GRP	Governance, Risk and Policy
GV.AT-P	Awareness and Training
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
ICMP	Internet Control Message Protocol
ID	Identify
ID.SC	Supply Chain Risk Management
IR	Incident Response Family
IRP	Incident Response Plan
IRS	Internal Revenue Service
ISO	Information System Owner
ISSO	Information System Security Officer
IT	Information Technology
L	Low
M	Moderate

Acronym	Definition
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
ODP	Organizationally Defined Parameters
OIG	Office of the Inspector General
OMB	Office of Management and Budget
P	Privacy
PF	Privacy Framework
PII	Personally Identifiable Information
PO	Principal Office
PR	Protect
PR.AT	Awareness and Training
PR.IP	Information Protection Processes and Procedures
PR.PO-P	Data Protection Policies, Processes, and Procedures
PR-P	Protect-P
PUB	Publication
RAF	Risk Acceptance Form
RC	Recover
RC.CO	Communications
RC.IM	Improvements
RC.RP	Recovery Planning
RS	Respond
RS.AN	Analysis
RS.CO	Communications
RS.IM	Improvements
RS.MI	Mitigation
RS.RP	Response Planning
SAOP	Senior Agency Official for Privacy
SP	Special Publication
SSN	Social Security Number
US-CERT	United States Computer Emergency Readiness Team
Wi-Fi	Wireless Fidelity

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
IR-01	Policy and Procedures	X	X	X	X	PR.IP, DE.DP, GV.PO-P, GV.MT-P, CM.AW-P, PR.PO-P	PR.IP-9, DE.DP-2, GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6, CM.AW-P7, PR.PO-P7
IR-02	Incident Response Training	X	X	X	X	PR.AT, GV.AT-P, CM.AW-P	PR.AT-5, GV.AT-P3, CM.AW-P7
IR-02(01)	Incident Response Training | Simulated Events				X	PR.AT, GV.AT-P, CM.AW-P	PR.AT-5, GV.AT-P3, CM.AW-P7
IR-02(02)	Incident Response Training | Automated Training Environments				X	PR.AT, GV.AT-P, CM.AW-P	PR.AT-5, GV.AT-P3, CM.AW-P7
IR-02(03)	Incident Response Training | Breach	X				PR.AT, GV.AT-P, CM.AW-P	PR.AT-5, GV.AT-P3, CM.AW-P7
IR-03	Incident Response Testing	X		X	X	ID.SC, PR.IP, RS.CO, PR.PO-P	ID.SC-5, PR.IP-7, PR.IP-10, RS.CO-1, PR.PO-P5, PR.PO-P8
IR-03(01)	Incident Response Testing | Automated Testing					ID.SC, PR.IP, RS.CO, PR.PO-P	ID.SC-5, PR.IP-7, PR.IP-10, RS.CO-1, PR.PO-P5, PR.PO-P8
IR-03(02)	Incident Response Testing | Coordination with Related Plans			X	X	ID.SC, PR.IP, RS.CO, PR.PO-P	ID.SC-5, PR.IP-7, PR.IP-10, RS.CO-1, PR.PO-P5, PR.PO-P8
IR-03(03)	Incident Response Testing | Continuous Improvement					ID.SC, PR.IP, RS.CO, PR.PO-P	ID.SC-5, PR.IP-7, PR.IP-10, RS.CO-1, PR.PO-P5, PR.PO-P8
IR-04	Incident Handling	X	X	X	X	ID.SC, DE.AE,	ID.SC-5, DE.AE-2,

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.RP, RS.CO, RS.AN, RS.MI, RS.IM, RC.RP, RC.IM, RC.CO, GV.MT-P, CM.AW-P	DE.AE-3, DE.AE-4, DE.AE-5, RS.RP-1, RS.CO-3, RS.CO-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, RC.CO-1, RC.CO-2, RC.CO-3, GV.MT-P6, CM.AW-P7
IR-04(01)	Incident Handling | Automated Incident Handling Processes			X	X	ID.SC, DE.AE, RS.RP, RS.CO, RS.AN, RS.MI, RS.IM, RC.RP, RC.IM, RC.CO, GV.MT-P, CM.AW-P	ID.SC-5, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS.RP-1, RS.CO-3, RS.CO-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, RC.CO-1, RC.CO-2, RC.CO-3, GV.MT-P6, CM.AW-P7
IR-04(02)	Incident Handling | Dynamic Reconfiguration					ID.SC, DE.AE, RS.RP, RS.CO, RS.AN,	ID.SC-5, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-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, RS.IM, RC.RP, RC.IM, RC.CO, GV.MT-P, CM.AW-P	RS.RP-1, RS.CO-3, RS.CO-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, RC.CO-1, RC.CO-2, RC.CO-3, GV.MT-P6, CM.AW-P7
IR-04(03)	Incident Handling | Continuity of Operations					ID.SC, DE.AE, RS.RP, RS.CO, RS.AN, RS.MI, RS.IM, RC.RP, RC.IM, RC.CO, GV.MT-P, CM.AW-P	ID.SC-5, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS.RP-1, RS.CO-3, RS.CO-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, RC.CO-1, RC.CO-2, RC.CO-3, GV.MT-P6, CM.AW-P7
IR-04(04)	Incident Handling | Information Correlation				X	ID.SC, DE.AE, RS.RP, RS.CO, RS.AN, RS.MI, RS.IM, RC.RP,	ID.SC-5, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS.RP-1, RS.CO-3, RS.CO-4,

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
						RC.IM, RC.CO, GV.MT-P, CM.AW-P	RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, RC.CO-1, RC.CO-2, RC.CO-3, GV.MT-P6, CM.AW-P7
IR-04(05)	Incident Handling | Automatic Disabling of System					ID.SC, DE.AE, RS.RP, RS.CO, RS.AN, RS.MI, RS.IM, RC.RP, RC.IM, RC.CO, GV.MT-P, CM.AW-P	ID.SC-5, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS.RP-1, RS.CO-3, RS.CO-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, RC.CO-1, RC.CO-2, RC.CO-3, GV.MT-P6, CM.AW-P7
IR-04(06)	Incident Handling | Insider Threats					ID.SC, DE.AE, RS.RP, RS.CO, RS.AN, RS.MI, RS.IM, RC.RP, RC.IM, RC.CO,	ID.SC-5, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS.RP-1, RS.CO-3, RS.CO-4, RS.AN-1, RS.AN-2, RS.AN-3,

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
						GV.MT-P, CM.AW-P	RS.AN-4, RS.MI-1, RS.MI-2, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, RC.CO-1, RC.CO-2, RC.CO-3, GV.MT-P6, CM.AW-P7
IR-04(07)	Incident Handling | Insider Threats — Intra-organization Coordination					ID.SC, DE.AE, RS.RP, RS.CO, RS.AN, RS.MI, RS.IM, RC.RP, RC.IM, RC.CO, GV.MT-P, CM.AW-P	ID.SC-5, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS.RP-1, RS.CO-3, RS.CO-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, RC.CO-1, RC.CO-2, RC.CO-3, GV.MT-P6, CM.AW-P7
IR-04(08)	Incident Handling | Correlation with External Organizations					ID.SC, DE.AE, RS.RP, RS.CO, RS.AN, RS.MI, RS.IM, RC.RP, RC.IM, RC.CO, GV.MT-P, CM.AW-P	ID.SC-5, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS.RP-1, RS.CO-3, RS.CO-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2,

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.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, RC.CO-1, RC.CO-2, RC.CO-3, GV.MT-P6, CM.AW-P7
IR-04(09)	Incident Handling | Dynamic Response Capability					ID.SC, DE.AE, RS.RP, RS.CO, RS.AN, RS.MI, RS.IM, RC.RP, RC.IM, RC.CO, GV.MT-P, CM.AW-P	ID.SC-5, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS.RP-1, RS.CO-3, RS.CO-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, RC.CO-1, RC.CO-2, RC.CO-3, GV.MT-P6, CM.AW-P7
IR-04(10)	Incident Handling | Supply Chain Coordination					ID.SC, DE.AE, RS.RP, RS.CO, RS.AN, RS.MI, RS.IM, RC.RP, RC.IM, RC.CO, GV.MT-P, CM.AW-P	ID.SC-5, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS.RP-1, RS.CO-3, RS.CO-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2, RS.IM-1, RS.IM-2, RC.RP-1,

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
							RC.IM-1, RC.IM-2, RC.CO-1, RC.CO-2, RC.CO-3, GV.MT-P6, CM.AW-P7
IR-04(11)	Incident Handling | Integrated Incident Response Team				X	ID.SC, DE.AE, RS.RP, RS.CO, RS.AN, RS.MI, RS.IM, RC.RP, RC.IM, RC.CO, GV.MT-P, CM.AW-P	ID.SC-5, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS.RP-1, RS.CO-3, RS.CO-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, RC.CO-1, RC.CO-2, RC.CO-3, GV.MT-P6, CM.AW-P7
IR-04(12)	Incident Handling | Malicious Code and Forensic Analysis					ID.SC, DE.AE, RS.RP, RS.CO, RS.AN, RS.MI, RS.IM, RC.RP, RC.IM, RC.CO, GV.MT-P, CM.AW-P	ID.SC-5, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS.RP-1, RS.CO-3, RS.CO-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, RC.CO-1,

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
							RC.CO-2, RC.CO-3, GV.MT-P6, CM.AW-P7
IR-04(13)	Incident Handling | Behavior Analysis					ID.SC, DE.AE, RS.RP, RS.CO, RS.AN, RS.MI, RS.IM, RC.RP, RC.IM, RC.CO, GV.MT-P, CM.AW-P	ID.SC-5, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS.RP-1, RS.CO-3, RS.CO-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, RC.CO-1, RC.CO-2, RC.CO-3, GV.MT-P6, CM.AW-P7
IR-04(14)	Incident Handling | Security Operations Center					ID.SC, DE.AE, RS.RP, RS.CO, RS.AN, RS.MI, RS.IM, RC.RP, RC.IM, RC.CO, GV.MT-P, CM.AW-P	ID.SC-5, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS.RP-1, RS.CO-3, RS.CO-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, RC.CO-1, RC.CO-2, RC.CO-3,

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
							GV.MT-P6, CM.AW-P7
IR-05	Incident Monitoring	X	X	X	X	ID.SC, DE.AE, RS.RP, RS.CO, RS.AN, RS.MI, RS.IM, RC.RP, RC.IM, RC.CO, GV.MT-P, CM.AW-P	ID.SC-5, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS.RP-1, RS.CO-3, RS.CO-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, RC.CO-1, RC.CO-2, RC.CO-3, GV.MT-P6, CM.AW-P7
IR-05(01)	Incident Monitoring | Automated Tracking, Data Collection, and Analysis				X	DE.AE, RS.AN	DE.AE-3, DE.AE-5, RS.AN-1, RS.AN-4
IR-06	Incident Reporting	X	X	X	X	DE.AE, RS.AN	DE.AE-3, DE.AE-5, RS.AN-1, RS.AN-4
IR-06(01)	Incident Reporting | Automated Reporting			X	X	RS.CO, CM.AW-P	RS.CO-2, CM.AW-P7
IR-06(02)	Incident Reporting | Vulnerabilities Related to Incidents					RS.CO, CM.AW-P	RS.CO-2, CM.AW-P7
IR-06(03)	Incident Reporting | Supply Chain Coordination			X	X	RS.CO, CM.AW-P	RS.CO-2, CM.AW-P7
IR-07	Incident Response Assistance	X	X	X	X	RS.CO, CM.AW-P	RS.CO-2, CM.AW-P7
IR-07(01)	Incident Response Assistance | Automation Support for Availability of Information and Support			X	X	PR.IP, CM.AW-P, PR.PO-P	PR.IP-9, CM.AW-P8, PR.PO-P7
IR-07(02)	Incident Response Assistance | Coordination with External Providers					PR.IP, CM.AW-P, PR.PO-P	PR.IP-9, CM.AW-P8, PR.PO-P7

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
IR-08	Incident Response Plan	X	X	X	X	PR.IP, CM.AW-P, PR.PO-P	PR.IP-9, CM.AW-P8, PR.PO-P7
IR-08(01)	Incident Response Plan | Breaches	X				ID.SC, PR.IP, DE.AE, RS.RP, RS.CO, RS.AN, RS.IM, RC.RP, RC.IM, CM.AW-P, PR.PO-P	ID.SC-5, PR.IP-7, PR.IP-8, PR.IP-9, DE.AE-3, DE.AE-5, RS.RP-1, RS.CO-1, RS.CO-2, RS.CO-3, RS.CO-4, RS.AN-4, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, CM.AW-P7, PR.PO-P5, PR.PO-P6, PR.PO-P7
IR-09	Information Spillage Response					ID.SC, PR.IP, DE.AE, RS.RP, RS.CO, RS.AN, RS.IM, RC.RP, RC.IM, CM.AW-P, PR.PO-P	ID.SC-5, PR.IP-7, PR.IP-8, PR.IP-9, DE.AE-3, DE.AE-5, RS.RP-1, RS.CO-1, RS.CO-2, RS.CO-3, RS.CO-4, RS.AN-4, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, CM.AW-P7, PR.PO-P5, PR.PO-P6, PR.PO-P7
IR-09(02)	Information Spillage Response | Training					ID.SC, PR.IP, PR.PO-P	ID.SC-5, PR.IP-9, PR.PO-P7

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
IR-09(03)	Information Spillage Response | Post-spill Operations					ID.SC, PR.IP, PR.PO-P	ID.SC-5, PR.IP-9, PR.PO-P7
IR-09(04)	Information Spillage Response | Exposure to Unauthorized Personnel					ID.SC, PR.IP, PR.PO-P	ID.SC-5, PR.IP-9, PR.PO-P7

APPENDIX B – REPORTING EVENTS

Incidents that may constitute a computer crime (violations of applicable Federal and/or State laws) must be reported to the OIG. Examples of the types of incidents that must be reported include, but are not limited to, the following:

Description	Example
Denial of Service (DoS)	CISA reports of DoS attacks on ED systems. Examples of DoS include, Buffer Overflow, Internet Control Message Protocol (ICMP) Flood, and SYN Flood attempts.
Unauthorized Access on internally and externally hosted systems, as well as Federal Student Aid (FSA) partner systems	Individuals intentionally trying to gain access to PII information, systems, or components that they do not authorization to access.
Exceeding authorized access (abuse of system privileges)	A system user uses his or her privileges to conduct unauthorized searches for loan information.
Criminal misuse of information technology (IT) resources	An employee who uses his or her government issued equipment to operate a business on government time and government laptop. Additional activities include, fraud, theft, hacking, and identify theft.
Illegal interception of electronic communications	An individual who set themselves up as proxy or delegate to get access to an executive's email account without their knowledge. The use of any electronic, mechanical, or other device to intercept communications transmitted by wire, cable, or radio, e.g., Man-in-the-Middle, unauthorized port mirroring/packet capture, and unauthorized proxies or Wireless Fidelity (Wi-Fi) hotspots with the intention of intercepting end-user traffic
Compromise of System or Application privileges (root access)	An external threat actor compromises an admin/root account on a system or application.
Compromise of information protected by law	During contract negotiations, a Department employee or contractor sends non-releasable contract or bid related information to their private, or their company, email address. When an employee's misconduct or administrative investigation (involving one or more employees) is being reviewed by management, and an individual then releases that information to the press or media without authorization private, or their company, email address. When an employee's misconduct or administrative investigation (involving one or more employees) is being reviewed by management, and an individual then releases that information to the press or media without authorization
Attempts to access child pornography	An individual is found to be accessing child pornography using Department systems.
Malicious destruction or modification of Department data and/or information	An example is when an individual is found to be maliciously deleting or modifying Department data without proper authorization, including Department data hosted at external partner systems (e.g., Servicers, Title IVs, and Schools).

Description	Example
Unauthorized Disclosure	A user accidentally sends an email of another individual's social security number (SSN) to the wrong email address. The user then self-reports the event to EDSOC. A user self-reports finding an unprotected document, configured without the proper security permissions, containing PII, such as Social Security numbers. The user informs EDSOC of his or her discovery. EDSOC conducts a review and determines only authorized users have access to the file.