Department of Homeland Security
Cybersecurity and Infrastructure Security Agency
Directives System
Directive Number: 3180 01-0.01
Issue Date: 12/29/2020

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY RECORDS AND INFORMATION MANAGEMENT PROGRAM

I. Purpose

This Directive establishes the Cybersecurity and Infrastructure Security Agency (CISA) Records and Information Management (RIM) Program.

II. Scope of Application

This Directive applies to all employees and contractors throughout CISA. This directive supersedes National Protection and Programs Directorate (NPPD) Directive 141-01 "Records and Information Management Program".

III. Authorities

A. Title 5 United States Code (U.S.C.) II, 552, 552a, and 553, "Administrative Procedure"
B. Title 18 U.S.C. 101, "Records and Reports"
C. Title 18 U.S.C. 121, "Stored Wire and Electronic Communications and Transactional Records Access"
D. Title 40 U.S.C. III, "Information Technology Management"
E. Title 44 U.S.C. 21, "National Archives and Records Administration" (NARA)
F. Title 5 Code of Federal Regulations (CFR) 1320, "Controlling Paperwork Burdens on the Public"
G. Title 36, CFR, Chapter XII, Subchapter B, "Records Management"
H. Title 41, CFR, Subtitle C, Chapter 102, "Creation, Maintenance, and Use of Records"
I. Title 44 U.S.C. 29, "Records Management by the Archivist of the United States and by the Administrator of General Services"
J. Title 44 U.S.C. 31, "Records Management by Federal Agencies"
K. Title 44 U.S.C. 33, "Disposal of Records"
L. Title 44 U.S.C. 35, "Coordination of Federal Information Policy"
M. Title 44 U.S.C. 36, "Management and Promotion of Electronic Government Services"
N. Office of Management and Budget (OMB) / NARA Memorandum M-19-21, "Transition to Electronic Records," June 28, 2019
O. Department of Homeland Security (DHS) Management Directive 141-01 (Rev 01), "Records and Information Management," August 11, 2014

IV. Definitions

A. **Agency Records Schedule**: A document approved by NARA that outlines when agency records that are not already covered by the General Records Schedule can be disposed of or transferred. Agencies develop this document in collaboration with NARA using Standard Form-115, "Request for Records Disposition Authority." NARA undertakes its review of agencies' Records Schedule disposition requests in four basic stages; receive, review, *Federal Register* notice and comment, and resolve.

B. **Disposal**: In federal usage, refers to only those final actions taken regarding temporary records after their retention periods expire.

C. **Electronic Records Management (ERM)**: The use of automated techniques to manage records regardless of format. ERM is the broadest term that refers to electronically managing records on varied formats (e.g., electronic, paper, microform, or other media).

D. **Essential Records**: Essential agency records required to meet operational responsibilities under national security emergencies or other emergency operating records. Essential agency records are used protect the legal and financial rights of the government and those affected by government activities (legal and financial rights records).

E. **Federal Records**: All recorded information, regardless of form or characteristics, that is:
   1. Made or received by a federal agency under federal law, or in connection with the transaction of public business, and
   2. Preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the U.S. Government or because of the informational value of data in them.

   This includes all traditional forms of records, regardless of physical form or characteristics, including information created, manipulated, communicated, or stored in digital or electronic form.

F. **File Plan**: A list of records in a specific office that describes how the records are organized and maintained.

G. **Privacy Impact Assessment (PIA)**: An analysis of how information is handled to:
   1. Ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy.
   2. Determine the risks and effects of creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and disposing of information in identifiable form in an electronic information system.
   3. Examine and evaluate protections and alternate processes for handling information to mitigate potential privacy concerns.

   A PIA is both an analysis and a formal document detailing the process and the outcome of the analysis.

H. **Privacy Threshold Analysis (PTA)**: Serves as the official determination as to whether the system, program, technology, form, or rulemaking is privacy sensitive (i.e., involves the collection and use of personally identifiable information (PII)) and requires additional privacy compliance documentation.

I. **Records Inventory**: List of all documents, files, and records created or received and maintained by an organization. It describes the title, function, purpose, content, date, format, recording media, and other important or relevant information, and helps in the development of an Agency Records Retention Schedule.

J. **Records Transfer**: A process that results in approved records storage facilities taking custody, but not ownership, of temporary and/or permanent agency records from CISA.

K. **System of Record Notice (SORN)**: Published by CISA in the *Federal Register* upon the establishment and/or modification of a system of records. Identifies the system of records, the purpose(s) of the system, the authority for maintenance of the records, the categories of records maintained in the system, the categories of individuals about whom records are maintained, the routine uses to which the records are subject, and additional details about the system.

V. Responsibilities

A. The **Director, CISA**:

1. Implements the CISA RIM Program across CISA.
2. Designates a Chief Records Officer to manage and implement a CISA RIM Program.

B. The **CISA Records Officer**:

1. Creates the CISA Records Schedules.
2. Approves the file plan and record inventory for each division and mission support office (office).
3. Develops and executes a plan to maintain essential records.
4. Develops records management training for CISA employees and contractors.
5. Develops on-boarding and off-boarding Records Management training for CISA employees.
6. Develops and delivers training for Records Liaisons Officers (RLOs) and Records Custodians (RCs)[2].
7. Gathers and reports annual metrics for the CISA RIM Program.
8. Manages the lifecycle for records retention, which includes the identification, capture and retention, transfer, and disposal of records.
9. Determines requirements and facilitates timely and accurate searches for requests for information.
10. Issues Instructions and other guidance to implement the requirements of this Directive.

[2] RCs support the RLOs within larger divisions and offices. They perform the same functions as the RLOs for the divisions but for their specific office.

C. The **Chief Information Officer (CIO)**:

1. Ensures CISA systems can capture and store electronic records and associated metadata in DHS enterprise-wide systems and applications in accordance with all applicable NARA, DHS, and CISA policies.
2. Ensures that systems administrators follow established NARA, DHS, and CISA policies for records management.

D. The **Chief Privacy Officer (CPO)**:

1. Works with the responsible division or office and the CISA RIM Program to ensure records containing PII are only retained for a reasonable amount of time so that mission objectives are met while preserving personal privacy.
2. Works with the CISA RIM Program, RLOs, and RCs to ensure that PII that is scheduled for disposition or transfer is processed in a timely manner.
3. Collaborates with the CISA RIM Program to ensure that records retention schedules are accurately documented in PTAs, PIAs, and SORNs.

E. The **Chief Human Capital Officer (CHCO)**:

1. Ensures RIM training is included as a component of the on and off-boarding procedures for all CISA employees.
2. Facilitates annual RIM training for CISA employees.

F. The **Chief of Procurement**:

1. Ensures RIM training is included as a component of the on and off-boarding procedures for all CISA contractors.
2. Facilitates annual RIM training for CISA contractors.
3. Ensures compliance with all applicable records retention schedules.

G. The **Chief Counsel**:

1. Provides notice to the CIO and other appropriate officials of the need to suspend records disposition requirements for litigation, congressional inquiries, etc. and when suspensions have been lifted.

H. The **Heads of Divisions and Mission Support Offices**:

1. Designate an RLO and RCs for larger divisions, offices, and regions.
2. Ensure adherence to the policies, procedures, and practices of the CISA RIM Program.
3. Ensure compliance with all applicable records retention schedules.

I. The **Records Liaison Officers and Records Custodians**:

1. Serve as the primary point of contact for records management within their office or division and as the liaison to the CISA RIM Program.
2. Sustain and refresh knowledge of records management and CISA's RIM Program.
3. Assist with the development of file plans and a record inventory for their respective division or office.
4. Update file plans and record inventory to ensure accessibility, accuracy, retrieval, storage, and disposition of records.

5. Coordinate records activities within their division or office and notify the CISA RIM Program of any noncompliance.
6. Report unauthorized removal, accidental or intentional deletion, damage, or loss of records to the CISA RIM Program.

VI. Requirements

A. Purpose

The CISA RIM Program ensures CISA complies with NARA and DHS requirements by setting records management standards and processes, and providing CISA's employees and contractors with records management expertise, guidance, and resources to support compliance.

B. Description

The CISA RIM Program establishes records management standards, executes the records management lifecycle, and facilitates training and outreach to CISA staff. These program elements equip CISA with agile, effective, and adaptive RIM resources to advance mission operations, increase accountability, preserve knowledge, and foster public trust. The elements of CISA's RIM Program are described below. Additional information on their implementation and execution is provided in their respective Instructions.

1. **Records Management Administration**
   The CISA RIM Program standardizes and unifies records management practices in compliance with NARA standards by creating structure and standards for records consistency through the following elements:

   a. **Records Schedule**: The CISA RIM Program creates and implements the CISA Records Schedule. The CISA Records Schedule is reviewed and approved annually by the Records Officer in coordination with NARA.

   b. **File Plans**: The RLOs and RCs ensure records within each office or division are listed in the file plan and are described accurately in the DHS Records Schedule. The CISA RIM Program ensures records are centralized, protected, and preserved; and the CIO, the RLOs, and the RCs ensure they are accessible and retrievable. File plans are developed for every division and office and combined in an overall CISA File Plan.

   c. **Essential Records**: In coordination with CISA continuity of operations working groups and plans, CISA's RIM Program works with RLOs and RCs to identify and maintain the federal and agency records necessary to maintain CISA's day-to-day operations in the event of a catastrophic or natural disaster. These records are accessible and retrievable at the DHS alternate operating facility.

   d. **Electronic Records**: The CISA RIM Program establishes standards to ensure electronic records are properly maintained for all CISA programs, projects, and administration efforts. The Records Officer coordinates with the CIO, the CPO, the RLOs, and the RCs to ensure these ERM standards are incorporated in all CISA electronic storage repositories (e.g., SharePoint, shared drives, and

OneDrive).

e. **Information Requests**: The CISA RIM Program facilitates Privacy Act requests, litigation or preservation holds, congressional inquiries, and other information requests as needed in coordination with the Chief Counsel, the CIO, and the CPO.

f. **Audit and Compliance Checks**: The CISA RIM Program conducts regular audits of each division and office to ensure compliance with CISA, DHS, and NARA requirements. CISA's Records Officer provides audit results and metrics on records management compliance to CISA leadership and DHS's RIM Program.

2. **Records Management Lifecycle**
The CISA RIM Program manages the identification, capture, filing, and disposal or transfer of records through the RLOs and RCs. Through this lifecycle, the CISA RIM Program maintains official records providing adequate and proper documentation as evidence of CISA activities in compliance with NARA and other federal requirements. Records are managed through the RLOs and the RCs with close management and oversight by the Records Officer.

a. **Identification**: The CISA RIM Program identifies what records need to be stored in compliance with NARA standards.

b. **Capture**: The CISA RIM Program establishes the process for RLOs and RCs to capture and maintain office records in the approved file plan.

c. **Filing**: The CISA RIM Program works with the RLOs and the RCs to ensure that all government records are listed in the office file plan and are described accurately in the DHS Records Schedule.

d. **Disposal or Transfer**: The RLOs ensure the prompt disposal of temporary records when their retention periods expire and the timely transfer of permanent records to NARA as authorized by the CISA Records Schedule.

3. **Training & Outreach**
Training provides CISA's employees and contractors with records management expertise, guidance, and resources to successfully preserve and access information. This ensures all CISA employees and contractors safeguard their documents in compliance with the standards set forth in this Directive and supporting Instructions. The CISA RIM Program works with CHCO to provide on and off-boarding training to CISA employees and contractors, and annual training to CISA employees and contractors. CISA's RIM Program also develops and provides training for designated RLOs and RCs to safeguard documents for their respective office or division in compliance with DHS's and CISA's records management requirements, as well as other federal requirements.

VII. Compliance and Enforcement

A. The standards established in this Directive and its Instructions ensure compliance with legislative and statutory requirements on records management. RIM ensures consistency

for implementation of all phases of the records lifecycle and helps CISA maintain public trust, protect continuity in the event of a disaster, avert congressional and public scrutiny, and protect the rights of the agency, its employees, and its customers.

B. The Records Officer provides guidance, tools, and resources for division and office heads so they can implement and execute CISA RIM Program requirements and ensure compliance within their organizations. Consequences of noncompliance include administrative escalation, and employees and contractors may be required to undergo retraining. The CISA RIM Program conducts regular audits of each division and office to ensure compliance with the standards and requirements established in this Directive and supporting Instructions.

C. Enforcement methodology and compliance procedures are incorporated into each Instruction and Standard Operating Procedures implementing this Directive. As sponsor for this Directive, the CISA Records Officer executes such activities. The CISA Records Officer reports compliance indicator results and issues with nonconformance to this Directive to the Enterprise Performance Risk Management System and to the Director.

VIII. Questions

Address any questions or concerns regarding this Directive to the Records Officer at (b) (6) [redacted].

Summary of Changes:

Section Reference	Type of Change	Concise Description	Author/Approving Authority (Name, Office/Division)	Date of Approval
Scope	*Administrative*	*Added in language noting that this Directive supersedes NPPD Directive 141-01 "Records and Information Management Program."*	*Monica Watkins, OCIO / Meghan Chiles, SPP*	*4/28/2025 5/1/2025*

12/29/2020

Brandon Wales, Acting Director
Cybersecurity and Infrastructure Security Agency

Date