The Road to CUI Governance

Reinforcing and Enabling Information Governance for Controlled Unclassified Information

February 20, 2020

CONTENTS

Executive Summary

Inconsistencies in Sensitive But Unclassified (SBU) policies have both endangered information and reduced necessary transparency. A uniform program for the management of sensitive, unclassified information is standardizing how information is handled and shared. The National Archives and Records Administration-implemented Controlled But Unclassified (CUI) program is addressing SBU issues and deficiencies. Individual agencies are responsible for following their guidance as applicable.

BRMi offers a four-phase approach as federal agencies seek ways to evaluate, recommend, and implement policy, organization, process, and technology improvements for CUI governance. It enables agencies to assess, design, execute, and sustain an improved CUI governance environment. Our approach for creating a target CUI governance environment and roadmap has empowered chief information officers, security officers, and other agency officials to achieve sustainable, real-world reform.

Inconsistent Policies and Disparate Practices

Historically, the U.S. federal government has shared information designated "Sensitive But Unclassified," or "SBU," according to agency-specific policies and practices. Across the federal government, there are a variety of markings, labels, and handling procedures for SBU information.[1] There are few

[1] Library of Congress, Federal Research Division; *LAWS AND REGULATIONS GOVERNING THE PROTECTION OF SENSITIVE BUT UNCLASSIFIED INFORMATION* (Washington, D.C.: September 2004)

government-wide policies or procedures that describe the basis on which an agency should assign a given designation and use SBU information consistently from one agency to another.[2]

Variability and Confusion

The variety of designations and policies has proven confusing for those on the producing/sending and consuming/receiving end of SBU information.[3] Each agency determines the designations and associated policies to apply to the sensitive information it develops or shares. There are currently over 100 different ways of characterizing SBU information.

Endangered Information and Reduced Transparency

Inconsistencies in SBU policies have both endangered information and reduced necessary transparency; the likelihood is higher for errors in designating, marking, handling and sharing. Disparate SBU practices have impeded the timeliness, accuracy, and flow of information.[4] The labeling of unclassified data affects accessibility. The result: materials may be unnecessarily restricted and improperly withheld *or* necessarily restricted but improperly released.

What Is "SBU?"

Sensitive But Unclassified (SBU) is a U.S. federal government designation for unclassified information that often requires strict controls over its distribution. SBU is a broad category of information that includes material covered by such designations as For Official Use Only (FOUO), Law Enforcement Sensitive (LES), and Critical Infrastructure Information (CII), among others. It also includes Internal Revenue Service materials like individual tax records, systems information, and enforcement procedures. Some categories of SBU information have authority in statute or regulation (e.g., CII) while others (e.g., FOUO) do not.

Reform to Standardize Information Handling and Sharing

Common definitions, designating and decontrolling bases and authorities, formats, marking, and dissemination procedures are expected to clarify SBU more broadly, achieve more consistent marking, improve information sharing, and better safeguard information. A uniform program for the management of sensitive, unclassified information is intended to standardize how information is handled and shared.

Ongoing CUI[5] reform is meant to effectively and efficiently address SBU issues and deficiencies, in that it will provide a common definition and standardize processes and procedures.

[2] Government Accountability Office, *INFORMATION SHARING: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information*, GAO-06-385 (Washington, D.C.: March 2006)

[3] Ben Bain, "Sensitive but unclassified category simplified" *FCW* (May 12, 2008)

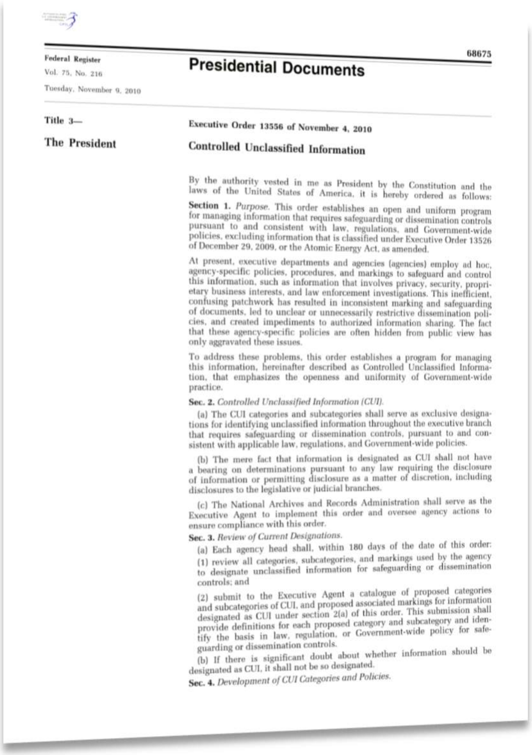
[4] Reports and Recommendations of the Presidential Task Force on Controlled Unclassified Information (Washington, D.C.: August 25, 2009)

[5] U.S. National Archives and Records Administration, Controlled Unclassified Information (CUI)

Government-Wide Management Policy

Executive Order 13556 established a program for government-wide CUI management and designated the National Archives and Records Administration (NARA) to implement and oversee said program.[6] The Information Security Oversight Office (ISOO) was charged with CUI management responsibilities.

Figure 1: CUI As Established by Executive Order 13556



Federal Register
Vol. 75, No. 216
Tuesday, November 9, 2010

68675

Presidential Documents

Title 3—

The President

Executive Order 13556 of November 4, 2010

Controlled Unclassified Information

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. *Purpose.* This order establishes an open and uniform program for managing information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, excluding information that is classified under Executive Order 13526 of December 29, 2009, or the Atomic Energy Act, as amended.

At present, executive departments and agencies (agencies) employ ad hoc, agency-specific policies, procedures, and markings to safeguard and control this information, such as information that involves privacy, security, proprietary business interests, and law enforcement investigations. This inefficient, confusing patchwork has resulted in inconsistent marking and safeguarding of documents, led to unclear or unnecessarily restrictive dissemination policies, and created impediments to authorized information sharing. The fact that these agency-specific policies are often hidden from public view has only aggravated these issues.

To address these problems, this order establishes a program for managing this information, hereinafter described as Controlled Unclassified Information, that emphasizes the openness and uniformity of Government-wide practice.

Sec. 2. *Controlled Unclassified Information (CUI).*

(a) The CUI categories and subcategories shall serve as exclusive designations for identifying unclassified information throughout the executive branch that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies.

(b) The mere fact that information is designated as CUI shall not have a bearing on determinations pursuant to any law requiring the disclosure of information or permitting disclosure as a matter of discretion, including disclosures to the legislative or judicial branches.

(c) The National Archives and Records Administration shall serve as the Executive Agent to implement this order and oversee agency actions to ensure compliance with this order.

Sec. 3. *Review of Current Designations.*

(a) Each agency head shall, within 180 days of the date of this order:

(1) review all categories, subcategories, and markings used by the agency to designate unclassified information for safeguarding or dissemination controls; and

(2) submit to the Executive Agent a catalogue of proposed categories and subcategories of CUI, and proposed associated markings for information designated as CUI under section 2(a) of this order. This submission shall provide definitions for each proposed category and subcategory and identify the basis in law, regulation, or Government-wide policy for safeguarding or dissemination controls.

(b) If there is significant doubt about whether information should be designated as CUI, it shall not be so designated.

Sec. 4. *Development of CUI Categories and Policies.*

The ISOO issued Title 32, Part 2002 of the Code of Federal Regulations (32 CFR 2002) regarding CUI.[7] This order established policy for all federal agencies regarding designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI, amongst other duties.

What Is "CUI?"

Executive Order 13556 establishes Controlled Unclassified Information (CUI) as "information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, excluding information that is classified under Executive Order 13526 of December 29, 2009, or the Atomic Energy Act, as amended".

Guidance and Applicability

NARA's guidance on CUI is very broad; it covers all federal agencies but not all controls are applicable to every agency in the federal government. There are scores of categories—currently 124—of CUI controls.[8]

Agency teams must determine the categories that are most applicable to a given agency, which may occur through interviews and/or surveys.

Stakeholder Buy-In

The CUI management program affects the workflow for all offices within the agency. Stakeholder buy-in is the key for its success.

At some agencies, the program's visibility has been increased by educating staff through targeted training sessions, policy updates, and

[6] Executive Office of the President, *Controlled Unclassified Information*, Executive Order 13556 (Washington, D.C.: November 2010)

[7] United States Government Publishing Office; Title 32, Part 2002, Year 2017 of the Code of Federal Regulations (32 CFR 2002)

[8] U.S. National Archives and Records Administration, CUI Categories

guides.[9]

Addressing Other Issues

Organizations may face other issues that need to be addressed. For example, inspectors general may recommend new measures for the protection of sensitive information.[10]

Organizations may need to satisfactorily address the findings of an inspection.

Assessing Maturity and Creating a Governance Roadmap

Per the CUI program, agencies are seeking ways to evaluate, recommend, and implement policy, organization, process, and technology improvements for CUI governance. To affect the reform intended by the CUI program, agencies should follow an approach with four phases:

1. *Assess* the information governance environment
2. *Design* a new environment for CUI management
3. *Execute* a transition between the past and future environments
4. *Sustain* the improved environment

The four phases are explained further, as follows.

Assessing Baseline Maturity

In the Assess phase, the focus is on

- Gathering data via surveys, interviews, and research;
- Comparing and analyzing gathered data; and
- Presenting results and findings.

The outcomes of the Assess phase are as follows:

- An understanding of the agency's current state of maturity at the enterprise and program office levels.
- Data-driven analyses of agency strengths and opportunities for improvement.

Common Signs of an Immature Program

Compliance varies among programs

Absence/disuse of a standardized storage location

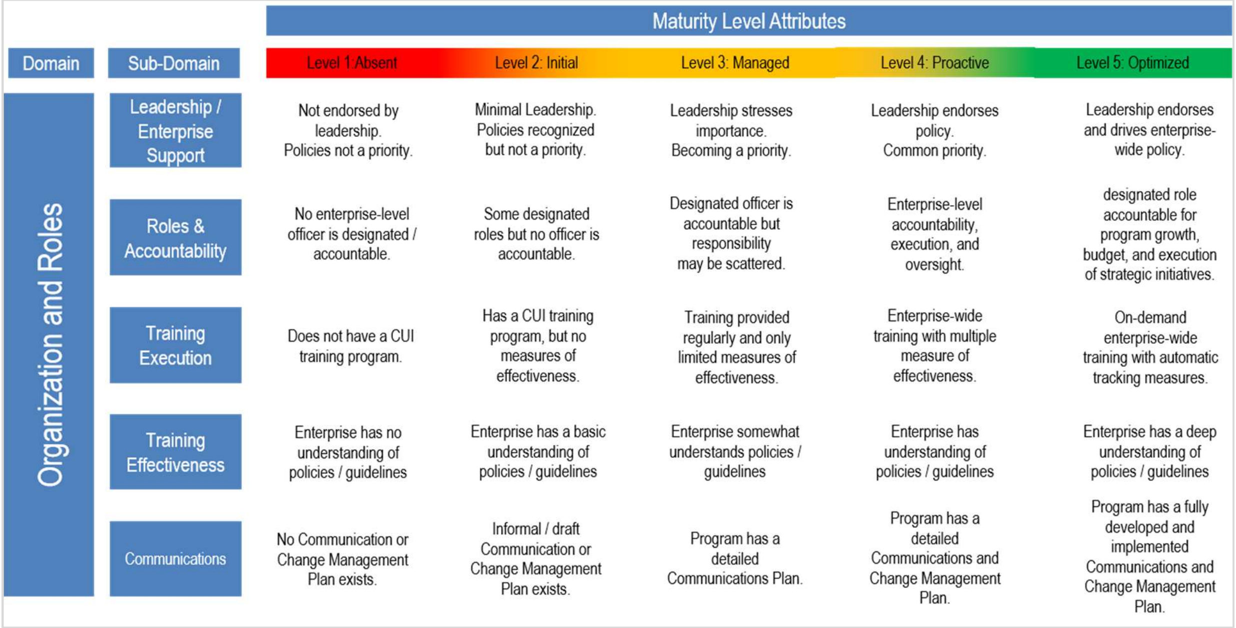
Gaps between staff understanding and execution

Figure 2 is an example of an information governance maturity model for a CUI program, a product of the Assess phase. Development of a maturity model provides insight into an organizational staff's ability to execute new standards and guidelines, as well as their participation and support for information governance.

[9] David Shive, Chief Information Officer, Office of GSA IT, General Services Administration; CIO Controlled Unclassified Information (CUI) Policy, CIO 2103.1 (Washington, D.C.: May 16, 2017)

[10] U.S. Department of Energy, Office of Inspector General, Office of Audits and Inspections; *INSPECTION REPORT: Review of Controls for Protecting Nonpublic Information at the Federal Energy Regulatory Commission*, DOE/IG-0933 (January 2015)

Figure 2: Maturity Model Attributes in the Organization-and-Roles Domain



		Maturity Level Attributes				
Domain	Sub-Domain	Level 1 Absent	Level 2: Initial	Level 3: Managed	Level 4: Proactive	Level 5: Optimized
Organization and Roles	Leadership / Enterprise Support	Not endorsed by leadership. Policies not a priority.	Minimal Leadership. Policies recognized but not a priority.	Leadership stresses importance. Becoming a priority.	Leadership endorses policy. Common priority.	Leadership endorses and drives enterprise-wide policy.
	Roles & Accountability	No enterprise-level officer is designated / accountable.	Some designated roles but no officer is accountable.	Designated officer is accountable but responsibility may be scattered.	Enterprise-level accountability, execution, and oversight.	designated role accountable for program growth, budget, and execution of strategic initiatives.
	Training Execution	Does not have a CUI training program.	Has a CUI training program, but no measures of effectiveness.	Training provided regularly and only limited measures of effectiveness.	Enterprise-wide training with multiple measure of effectiveness.	On-demand enterprise-wide training with automatic tracking measures.
	Training Effectiveness	Enterprise has no understanding of policies / guidelines	Enterprise has a basic understanding of policies / guidelines	Enterprise somewhat understands policies / guidelines	Enterprise has understanding of policies / guidelines	Enterprise has a deep understanding of policies / guidelines
	Communications	No Communication or Change Management Plan exists.	Informal / draft Communication or Change Management Plan exists.	Program has a detailed Communications Plan.	Program has a detailed Communications and Change Management Plan.	Program has a fully developed and implemented Communications and Change Management Plan.

The model separates maturity into domains and subdomains and ranks maturity in five levels: (1) absent, (2) initial, (3) managed, (4) proactive, and (5) optimized. It represents domains such as Organization and Roles, Strategy and Performance, Governance, and CUI Lifecycle. Maturity level attributes are identified according to sub-domains.

From this detailed maturity model, an appropriate target state with an achievable roadmap is possible.

Designing the Target State

In the Design phase, the focus is on

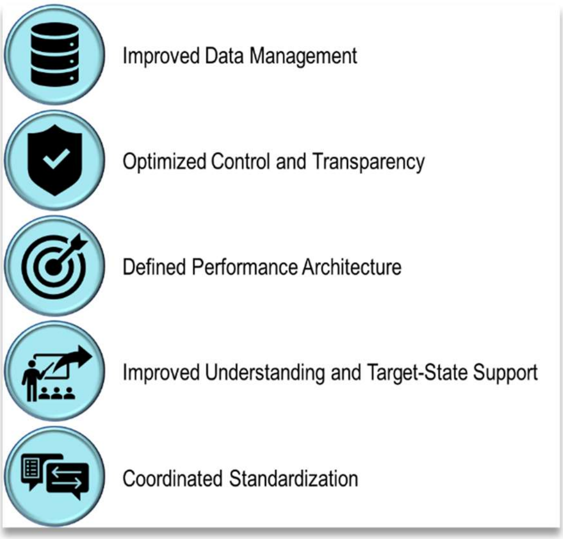
- Developing recommendations to mature governance based on key findings from the Assess phase and
- Creating a roadmap to specify the path and sequence to the target state.

While the final target-state may vary depending on the organization's maturity level, organizations often share common capabilities. Designing the best target state for an organization considers its structure, resources, and tools.

The outcomes of the Design phase are as follows:

- Governance informed by best practices, industry principles and pertinent standards.

Figure 3: Example of Proposed Capabilities

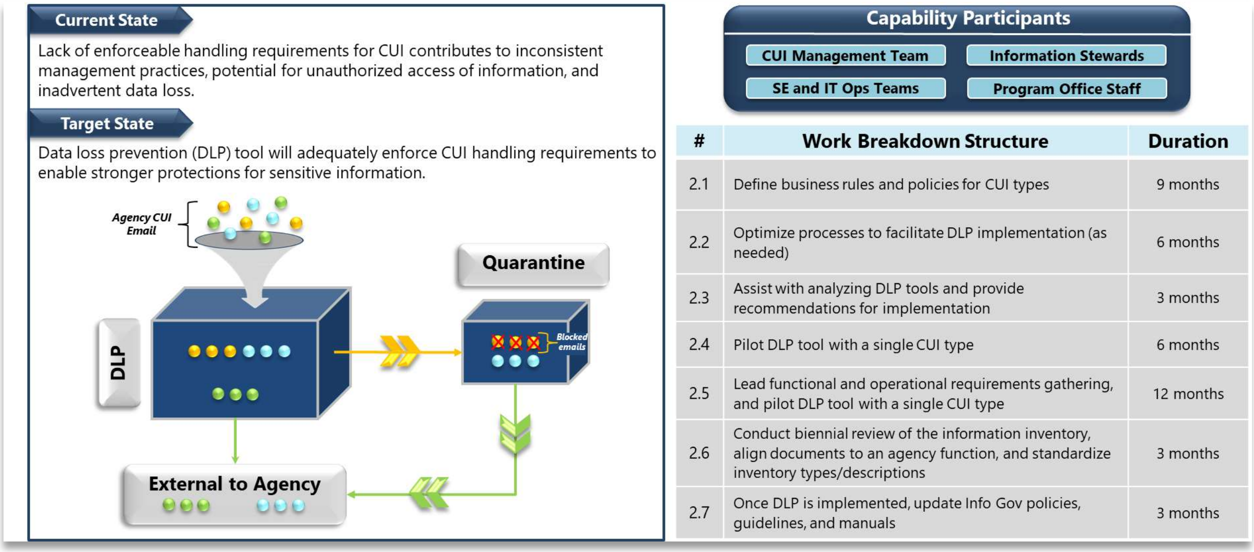


Improved Data Management
Optimized Control and Transparency
Defined Performance Architecture
Improved Understanding and Target-State Support
Coordinated Standardization

- Proposed capabilities (see Figure 3) that are relevant to findings from the Assess phase, tangible, and achievable.
- Specific recommendations to achieve proposed capabilities; the enterprise tools to plan personnel and resources.
- A roadmap specifying the path and sequence for each proposed capability; a longer-term view of the sequence of projects.

Each enterprise roadmap is tailored to required deadlines, resources, budget, and time. The roadmap also reflects each activity's duration, sequence, and dependencies.

Figure 4: Sample Work Breakdown Structure for a Proposed Capability



Current State

Lack of enforceable handling requirements for CUI contributes to inconsistent management practices, potential for unauthorized access of information, and inadvertent data loss.

Target State

Data loss prevention (DLP) tool will adequately enforce CUI handling requirements to enable stronger protections for sensitive information.

Capability Participants

CUI Management Team

Information Stewards

SE and IT Ops Teams

Program Office Staff

#	Work Breakdown Structure	Duration
2.1	Define business rules and policies for CUI types	9 months
2.2	Optimize processes to facilitate DLP implementation (as needed)	6 months
2.3	Assist with analyzing DLP tools and provide recommendations for implementation	3 months
2.4	Pilot DLP tool with a single CUI type	6 months
2.5	Lead functional and operational requirements gathering, and pilot DLP tool with a single CUI type	12 months
2.6	Conduct biennial review of the information inventory, align documents to an agency function, and standardize inventory types/descriptions	3 months
2.7	Once DLP is implemented, update Info Gov policies, guidelines, and manuals	3 months

Executing the Plan

In the Execute phase, the focus is on

- Developing a team, assigning resources and setting up tracking systems, and
- Executing a project plan in accordance with the Target State and Roadmap.

The outcomes of the Execution phases are as follows:

- Agency staff are trained and apply the CUI program as a part of their workflow.
- Agency is in full compliance with regulations and guidance from the ISOO.

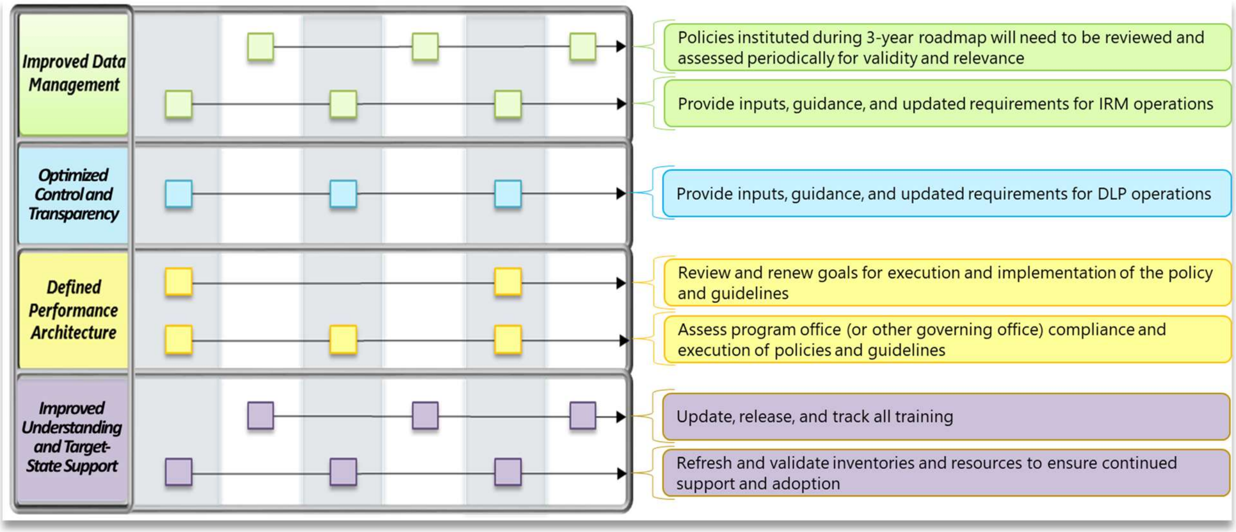
Sustaining the CUI Process

In the Sustain phase, the focus is on

- Assuring compliance with overseers (e.g., an information security oversight office),
- Training the agency staff, and
- Updating CUI inventory for offices.

Figure 5 presents a high-level timeline of some of the activities that can be expected to sustain the CUI process.

Figure 5: Sample Activities for Sustainment


Improved Data Management
Policies instituted during 3-year roadmap will need to be reviewed and assessed periodically for validity and relevance
Provide inputs, guidance, and updated requirements for IRM operations
Optimized Control and Transparency
Provide inputs, guidance, and updated requirements for DLP operations
Defined Performance Architecture
Review and renew goals for execution and implementation of the policy and guidelines
Assess program office (or other governing office) compliance and execution of policies and guidelines
Improved Understanding and Target-State Support
Update, release, and track all training
Refresh and validate inventories and resources to ensure continued support and adoption

Sustainable Reform with the Four-Phase Approach to Information Governance

BRMi's four-phase governance approach provides actionable and incremental reform for Controlled Unclassified Information in accordance with NARA guidance. Assessing the information governance environment through surveys, interviews, and research and using data-driven analyses in designing a new environment for CUI management results in greater stakeholder buy-in and a process for directly addressing other CUI issues.

By continuing to mature CUI governance through BRMi's four-phase approach, clients can more predictably become a compliant agency in the drive for government-wide CUI management, sustain reforms, and respond to operational/business demands on CUI, including inspector general findings.

Full implementation of standardized CUI governance enables clients to achieve more consistent marking, improve information sharing, and better safeguard information. This affects materials being necessarily restricted and properly withheld as well as necessarily unrestricted and properly released.

The four-phase approach for creating a target CUI governance environment and roadmap empowers chief information officers, security officers, and other agency officials to achieve real-world reform. With leadership commitment, BRMi can help clients achieve effective CUI management.

Mature Information Governance

BRMI's onsite team worked with a federal regulatory agency's Chief Information Security Officer and Information Governance Program Manager to develop an information governance program that oversees and implements the requirements

> "I am so proud of the work your team has done with the program and your leadership of all the related efforts…Job well done!!"
>
> Executive Director

enabling the protection of CUI and records management.

We supported the development of policy, guidelines, and an agency-wide training video. Our baseline assessment included a survey of randomly selected staff, 100+ interviews with stakeholders from 12 program offices, plus internal research.

> “The level of detail and thought put into the model and presentation far exceeded my expectations.”
>
> Chief Information Security Officer

We successfully designed the information-governance target-state based on our analysis, the execution of which has led to improvements in information sharing and safeguards.

Achieve Compliance for Better Management

BRMi assisted a federal administrative agency with management of records, including the establishment of a governance model. Following an assessment, which included input gathered from key stakeholders and the records management community at large, we designed a model that outlined and defined the structures overseeing the execution of records management. The governance model also included a roadmap and transition plan to plot the mechanics of adoption and continuous improvement.

We helped create a document with six sections based upon the lifecycle of electronic records management: (1) Capture, (2) Metadata, (3) Maintenance and Use, (4) Disposal, (5) Transfer, and (6) Reporting. Each section is controlled by a master requirement, which directs federal agencies to observe all guidelines relating to access rights and information controls. Individual sections described the governance committees, reporting mechanisms, and performance criteria to measure the success of implementation.

We further organized the bodies within the model into three levels with varying responsibilities and contributions. The executive level approves final products and process and policy changes. The advisory level provides guidance and direction on developing strategies for records management, as well as an access point for internal and external stakeholder feedback. The operational level creates the day-to-day products and deliverables.

Manage Information Across an Enterprise

A BRMi-led program management office (PMO) assisted a federal department in developing an overall information governance strategy to produce policy, procedures, and guidance necessary to advance records and information management across the enterprise. We reported on the state of records and information management across the department and created a progression model for the creation of a management program.

The PMO also supported the application of technology for information governance, coordinating the program within the department and with outside parties, supporting interagency records and information governance groups, and assisting records programs across the department with advice and technical expertise.

Let's talk more about sustainable CUI governance reform in your agency through BRMi's four-phase approach.

Ask us about scheduling an introductory meeting!

8403 Colesville Rd, Suite 260
Silver Spring, MD 20910

info@brmi.com

(301) 547-3324