POLICY ISSUE
(Information)

March 8, 2018 SECY-18-0035

FOR: The Commissioners

FROM: Victor M. McCree
Executive Director for Operations

SUBJECT: UPDATE ON DEVELOPMENT OF THE CONTROLLED UNCLASSIFIED INFORMATION PROGRAM

PURPOSE:

The purpose of this paper is to inform the Commission of the staff's approach to implementing Title 32 of the *Code of Federal Regulations* (32 CFR) Part 2002, "Controlled Unclassified Information (CUI)" (CUI Rule), including the staff's assessment of implementation activities, key milestones, and current schedule.

SUMMARY:

To implement the Governmentwide CUI Rule, the staff established an interoffice working group to examine potential issues and impacts related to the CUI Rule on the U.S. Nuclear Regulatory Commission (NRC) and its stakeholders, and to develop a strategy and approach for agency implementation. The implementation approach includes careful coordination with internal and external stakeholders; maximizes the use of existing policies, processes, and tools; draws on lessons learned from Executive Branch agencies; and minimizes burdensome and unintended consequences for stakeholders. The staff plans to implement the CUI Rule over the next 3.5 years. Although this schedule exceeds the initial implementation guidelines of the U.S. National Archives and Records Administration (NARA), it is consistent with the implementation schedules of most Federal agencies and enables the staff to apply a deliberate, well-informed approach in developing the policy.

CONTACT: Margie A. Janney, OCIO/GEMS
301-415-7245

BACKGROUND:

On September 14, 2016, NARA published the CUI Rule,[1] standardizing how the Executive Branch will handle sensitive unclassified information that requires safeguarding or dissemination controls. The CUI Rule went into effect on November 14, 2016, and established requirements for CUI designation, safeguarding, dissemination, marking, decontrolling, destruction, incident management, self-inspection, and oversight. The CUI Rule applies directly to Federal Executive Branch agencies, including the NRC. It applies indirectly, through agreements, to non-Executive Branch entities that have access to information designated as CUI. CUI does not include information that has been classified pursuant to an Executive Order or the Atomic Energy Act of 1954, as amended, or information a non-Executive Branch entity (e.g., contractors, licensees, Agreement States, intervenors) possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an Executive Branch agency or an entity acting for such an agency. The CUI Program at the NRC will replace the current Sensitive Unclassified Non-Safeguards Information (SUNSI) program (i.e., proprietary information, personally identifiable information) and include Safeguards Information (SGI) and Safeguards Information—Modified Handling.[2]

NARA recommends an implementation process for agency compliance with the CUI Rule that includes developing and issuing an agency CUI policy, creating agency CUI training, implementing and verifying that all physical safeguarding requirements are in place to protect CUI, providing CUI training to all agency employees, assessing and transitioning the current configuration of information systems to the CUI Rule standard, and developing and implementing internal oversight efforts to measure and monitor the CUI Program. Shortly after the rule became effective, NARA issued implementation guidelines indicating that agencies should issue policies within 180 days of the rule's effective date and complete full implementation within 2 years.[3] Based on Governmentwide feedback, NARA's current expectation is that most Federal agencies will publish agency-specific policies in summer 2018 and fully implement CUI Programs within the next 3 to 4 years. Agencies must submit to NARA an annual report on the status of CUI implementation.

DISCUSSION:

Staff Approach to Implement the CUI Rule

The CUI Rule establishes specific requirements for sensitive information that differ from those under the current SUNSI program, such as requirements for handling documents, incident management, self-inspection, and oversight activities. To facilitate the transition from SUNSI to CUI, the staff intends to apply the following principles: (1) minimize changes and burden to NRC staff and external stakeholders while complying with the CUI Rule, (2) ensure an open and transparent process, (3) implement the new CUI Program within the average timeframe

[1] NARA promulgated the CUI Rule in 32 CFR Part 2002 (Volume 81 of the *Federal Register* (FR), page 63,324 (81 FR 63324)). NARA issued the CUI Rule to implement Executive Order 13556, "Controlled Unclassified Information," which the President issued on November 4, 2010. The Executive Order established a program to standardize the way that the Executive Branch handles unclassified information that requires safeguarding or dissemination controls and it designated NARA as the CUI Executive Agent to implement that program.

[2] As discussed in the enclosure to this paper, the CUI Rule defers to existing information control requirements found in laws, regulations, and Governmentwide policies, such as those in 10 CFR Part 73, "Physical Protection of Plants and Materials," that apply to SGI. The CUI Rule generally will, however, supplant sensitive unclassified information controls identified only in agency-specific policies not codified in regulations.

[3] CUI Notice 2016-01: Implementation Guidance for the Controlled Unclassified Information Program

expected for most Federal agencies, and (4) work with NARA and other agencies to assess guidance and tools developed by other agencies that could inform the NRC's implementation plan.

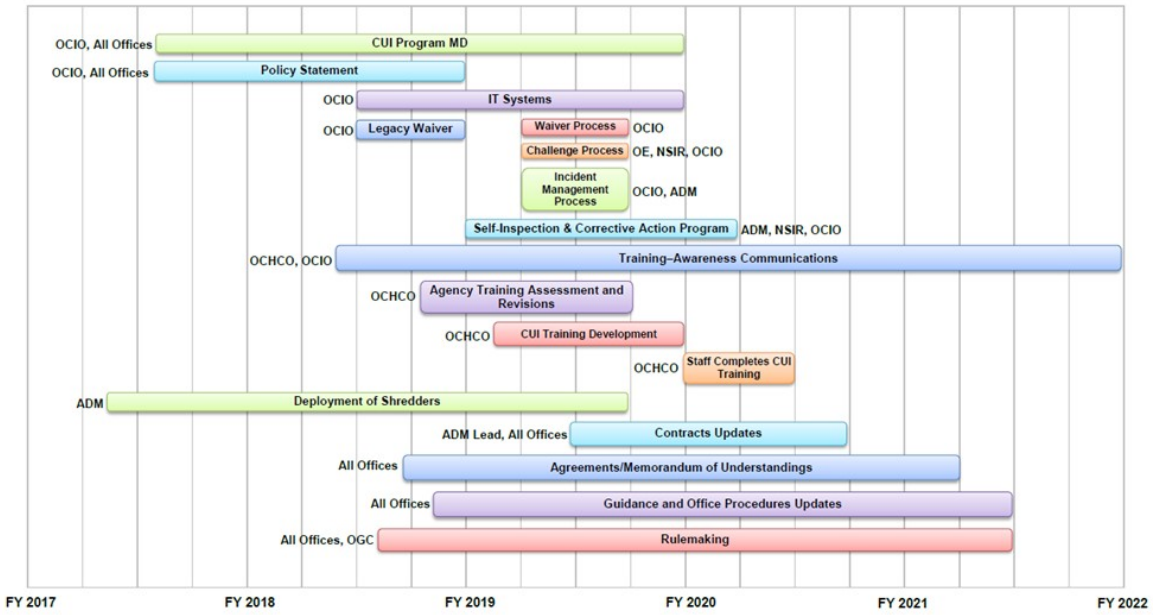
In alignment with these principles, the staff's approach to implementing the CUI Program is to: (1) leverage the NRC's SUNSI and SGI programs' policies, processes, and procedures to the extent practicable and (2) engage the NRC staff and external stakeholders to communicate the CUI Rule requirements, learn about any potential challenges that may result from the rule's implementation, and address challenges proactively. The staff believes that this approach will allow for effective coordination with stakeholders and minimize unintended consequences, while still implementing the CUI Rule on a schedule that is comparable with that of other Federal agencies.

An interoffice CUI Program working group, led by the Office of the Chief Information Officer (OCIO), is developing a CUI policy for Commission review and approval and has established an implementation plan through a collaborative and transparent process. The working group includes members who routinely work with SUNSI and collectively possess a thorough understanding of NRC policies, management directives (MDs), rules, regulations, external stakeholder interfaces, and Governmentwide policies and practices. To assess the differences between the NRC's SUNSI Program and the CUI Rule requirements, the working group completed a gap analysis comparing existing NRC SUNSI categories with approved categories in NARA's online CUI Registry.[4] Through the gap analysis, the working group identified implementation activities that will be needed for CUI Rule compliance and potential issues that will meaningfully change how the NRC staff and external stakeholders handle information.

Implementation Activities

To achieve implementation of the CUI Program by the end of fiscal year (FY) 2021, OCIO, in collaboration with NRC offices, developed a multi-project implementation plan that will take approximately 3.5 years to complete. The plan outlines the implementation activities that are essential to implement the CUI Program, as specified by the CUI Rule, and with as little disruption to staff and external stakeholders as practical. The implementation plan schedule will be impacted by the evolution of guidance released by NARA as well as resources that are available within the agency. The figure below shows the activities that offices will complete and the anticipated timeframes for completion. The graphical representation is based on a detailed draft project plan that identifies the tasks to be accomplished by each office. Lead offices are indicated although it is the intention for activities to be completed in a collaborative manner. The staff intends to further refine the schedule over the next few months. A summary of key implementation activities follows the figure.

[4] The *CUI Registry* is an online repository that identifies all approved CUI categories and subcategories, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes guidance on handling procedures, as well as other information.



Policy Development

NARA requires agencies to develop a CUI policy that addresses specific elements of the CUI program. The NRC staff intends to develop a CUI Policy Statement for the Commission's review and approval that would provide a high-level description of the NRC's approach to comply with the CUI Rule. Agency Management Directives (MDs) and other guidance and internal control documents will include detailed implementation guidance. The staff is actively developing the draft policy statement and intends to provide it to the Commission by September 2018.

Developing and Revising Guidance

In FY 2017, the staff started to revise MD 12.6, "NRC Sensitive Unclassified Information Security Program," dated December 20, 1999, to provide effective processes and guidance to implement the CUI Rule. The working group's understanding of the NRC's day-to-day operations was crucial for the revision of MD 12.6 so that the document will be consistent with the CUI Rule requirements.

The working group identified areas that led to further discussions and decision-making meetings to determine the best implementation approach. An example of one of the challenges that the staff is working through is that the CUI Registry does not contain all of the NRC's current SUNSI categories such as "Sensitive Internal Information – Sensitive" and "Predecisional." The staff is working with NARA to understand options for maintaining appropriate protections on these types of information.

The revised MD will capture the working group's recommendations that are meant to ensure that the NRC meets the intent of the CUI Rule with minimal impacts to the staff's day-to-day operations. Alignment on MD 12.6 will allow all offices to plan and initiate work on specific implementation activities, including the identification and revision of other MDs and associated office instructions and procedures by the middle of FY 2021.

Training

Employees who handle or create sensitive information must maintain a satisfactory knowledge and understanding of the protective measures that prevent or deter disclosures to unauthorized persons. The Office of the Chief Human Capital Officer (OCHCO) plans to leverage NARA's training modules and include the specifics of the NRC's CUI Program described in MD 12.6 when developing the agency CUI training. In addition, the staff is reviewing existing agency training modules and awareness products that describe protective measures for sensitive information within the agency and will update these tools as necessary. The staff is also participating in NARA's CUI training development working group. In an effort to begin preparing staff for the transition to CUI, OCIO, in collaboration with OCHCO, will hold awareness training for staff through internal communication activities (e.g., presentations at all-hands meetings, information tables, and agency-wide presentations) beginning in FY 2018. Formal, required training, such as a module in an online training course, will be introduced to the staff during FY 2020.

Physical Safeguards

The CUI Rule requires minimum physical safeguards to protect CUI in electronic and physical environments that are different than the NRC's current SUNSI requirements. For example, when hard copy CUI (e.g., paper, microfiche) is not under an authorized holder's direct control, it must be protected with at least one physical barrier that provides reasonable assurance that the CUI will be protected from unauthorized access or observation. This requirement may necessitate that all CUI be secured (e.g., locked from access) when it is not in the possession of an authorized user of the information. Staff will continue to evaluate this area as it develops revisions to MD 12.6, which will provide guidance to the staff on how to handle hardcopy CUI during work hours and while teleworking to prevent unauthorized access or observation as required by the CUI Rule.

Another safeguarding requirement is to control access to information to ensure that unauthorized individuals[5] cannot see, hear, or otherwise access CUI. The NRC's SUNSI policy requires similar controls for SUNSI information based on the need-to-know requirement. However, the CUI Rule may require changes to agency practices with regard to the discussion of sensitive information in cubicles. The preamble to the CUI Rule responds to questions on this topic and indicates that in a cubicle environment, it may be appropriate for agencies to segregate some employee operations from others and possibly reconfigure space. The Office of Administration (ADM) reviewed current protective measures, plans for renovations of physical workspaces and floors, and current policies, to identify policies, procedures, and practices that can be leveraged to comply with CUI physical safeguarding requirements. Although no changes to physical workspaces are anticipated, agency staff members will be encouraged to comply with the existing need-to-know policy, to use huddle rooms, and to be aware of their immediate environment and the people working around them who may not meet the need-to-know requirement for the information being discussed or reviewed. Additionally, the staff will be encouraged to use an enclosed space, if available, to conduct meetings or discussions involving sensitive information. The current policies and practices related to SGI will not change.

[5] Under the CUI Rule (32 CFR 2002.16, "Accessing and Disseminating"), CUI should be disseminated to, and accessed by, only those whose access "[f]urthers a lawful government purpose," is consistent with "the laws, regulations, and Governmentwide policies that" support treating the information as CUI, is not contrary to an applicable CUI limited dissemination control, and is not otherwise unlawful.

Destruction Standards

The CUI Rule requires that information that is controlled and unclassified, including in electronic form, be destroyed in a manner that makes the information unreadable, indecipherable, and irrecoverable. These destruction standards established by the CUI Rule are more stringent than the standards for the destruction of SUNSI and SGI. In June 2017, ADM completed a review of the CUI Rule requirement and analyzed the different options for complying with it. ADM determined that the most cost-effective approach for the agency was to install shredders that comply with requirements for the paper destruction of all CUI, SGI, and classified information. The installation of these shredders is in progress at NRC Headquarters and will be completed during FY 2019 for the entire agency, including the regional and resident inspector offices. Once shredders have been installed throughout the agency, burn bins will be removed from use, building by building. The current practice for the destruction of electronic media will remain unchanged. As described in MD 12.1, "NRC Facility Security Program," dated September 28, 2016, the staff will continue to provide sensitive electronic media such as hard drives, CDs, DVDs, diskettes, and flash drives to the ADM Division of Facilities and Security for appropriate destruction.

Legacy Waiver

To avoid the burdensome task of re-marking all sensitive information under the CUI requirements, each agency's Senior Agency Official[6] (SAO) has the authority to approve an agency-wide legacy waiver for documents created before the establishment of the agency CUI Program. The staff intends to recommend to the SAO the granting of such a waiver because remarking all documents created before the rule would be exceptionally resource intensive with no practical benefit. The waiver memorandum to program offices will describe the purpose of the legacy waiver and provide guidance to the staff to assure compliance with the CUI Rule. For example, if a document or portion of a document is reused for an agency purpose or is sent outside the agency, the CUI Rule requires that the document be appropriately marked as CUI to reflect the appropriate control. The waiver memo will be developed in FY 2018 and will be referenced in MD 12.6.

Waiver Process

In urgent circumstances, the NRC Senior Agency Official may waive the requirements of the CUI policy or the CUI Registry for any CUI within the NRC's possession or control, unless specifically prohibited by applicable laws, other regulations, or Governmentwide policies. OCIO will create a process and appropriate guidance for the staff for processing a waiver request under special circumstances. OCIO will lead this effort during FY 2019.

Incident Management Process

A key element of the CUI Program is incident reporting which includes the tracking and analysis of trends and patterns, as well as reporting and responding to the possible loss or compromise of CUI. Currently, the NRC has a SUNSI incident reporting process for employees that is managed by OCIO. There are two modes for reporting the mishandling or misuse of sensitive information electronically or physically. OCIO responds to the electronic misuse or electronic mishandling of sensitive information and ADM responds to the physical misuse or physical

[6] The NRC's Senior Agency Official for CUI is currently designated as the Director of the Governance and Enterprise Management Services Division in OCIO.

mishandling of sensitive information. OCIO and ADM plan to leverage the existing system and processes to incorporate the CUI incident management process in FY 2019 to ensure that the program adequately tracks and analyzes incidents such that trends and patterns can be appropriately identified and addressed consistent with the CUI Rule requirements.

Challenge Process

As required by the CUI Rule, the staff will develop CUI challenge procedures for information that has been designated as CUI by the NRC but that an authorized holder (Federal Government or non-Federal entity) believes is inappropriately designated as CUI, is not designated in accordance with CUI requirements, or is designated under an incorrect category within the CUI framework. The challenge procedures will provide an opportunity for the challenger to define a rationale for his or her belief that the CUI in question is inappropriately designated, an acknowledgement of receipt, an expected timetable for response to the challenger, and an identification of an appeal process with the appropriate guidance for submittal. Leveraging existing processes that may be similar and managed by the Office of Enforcement (OE) and the Office of Nuclear Security and Incident Response (NSIR), OCIO intends to develop the process during FY 2019.

Self-Inspection and Corrective Action Program

The CUI Rule requires agency establishment of a self-inspection program to monitor the CUI Program. To comply with this requirement, the NRC will need to review and assess the CUI Program to evaluate program effectiveness, measure the level of compliance, and monitor implementation efforts on an annual basis. In addition, the self-inspection program will include a corrective action program to monitor and track actions taken to address identified deficiencies. ADM and NSIR have experience in developing and overseeing such programs for classified information. Therefore, during FY 2019 OCIO will work collaboratively with ADM and NSIR to analyze NARA's reporting requirements and develop the appropriate procedures and processes for the CUI self-inspection program. In addition, OCIO will determine, in coordination with NSIR, the resources that will be necessary to carry out this activity once the CUI Program is implemented.

NRC Information Systems and Information Controls

Implementation of the CUI Rule will require assurance that agency information systems meet the CUI Rule cybersecurity control requirements. The agency may need to update internal processes and systems to ensure appropriate security controls for processing, transmitting, and storing CUI and, to ensure that printers, scanners, copiers, and fax machines do not retain data after use. The staff has developed a draft System Implementation Plan to identify systems and current regulatory guidance that would need to be updated to reflect the new requirements. The plan describes tasks and deliverables to ensure that all NRC systems employ cybersecurity controls consistent with the CUI Rule and applicable National Institute of Standards and Technology requirements. OCIO is leading this effort for the information systems under the corporate umbrella. However, in FY 2019, OCIO will work with the offices to assess the actions required for mission support information technology systems and make appropriate modifications in FY 2020. The staff has already updated MD 12.5, "NRC Cybersecurity Program," dated November 2, 2017, to account for the CUI Rule.

External Stakeholder Agreements

Although the CUI Rule only applies directly to Executive Branch agencies, whenever an agency intends to share CUI with a non-Executive Branch entity (e.g., contractors, licensees, Agreement States, tribes, intervenors), the CUI Rule states that an agency should, when feasible, enter into or modify existing agreements with those entities before sharing CUI. These agreements must include provisions that require the non-Executive Branch entity to handle CUI that is shared with them in accordance with the CUI Rule.[7] OCIO, in collaboration with all NRC offices, is exploring avenues to minimize the burdensome task of creating individual agreements with each NRC external stakeholder. The staff is exploring options to efficiently communicate the NRC's expectations for handling and protecting CUI. Interactions with external stakeholders will be crucial to provide clarity on the rule requirements and the agency's CUI Program.

NRC contractors who handle CUI will need to comply with standards set forth in the CUI Rule. ADM, in collaboration with NRC offices, will assess current and potential contracts to determine the degree of modifications required for contractors to meet CUI Rule requirements. The staff is awaiting an update to the Federal Acquisition Regulation, which NARA has indicated could be provided as early as spring 2018 and will then take at least a year before it is finalized.

A specific concern was raised by industry stakeholders at a recent public meeting regarding the treatment of information (e.g., floorplans, drawings) that was redacted out of final safety analysis reports at either the request of the licensee or at the request of the NRC. Licensees may not necessarily consider such information to be sensitive information needing special controls, and consequently, they may provide such information in the form of training and work instructions to employees, contractors and temporary workers. According to these stakeholders, the CUI Rule may create uncertainty as to whether these internal licensee documents—which have neither been shared with nor received from the NRC, but relate to information the NRC has designated as CUI in a different document—must nonetheless be protected to the same extent as CUI. As stated in the CUI Rule preamble, such information would not meet the definition of CUI because CUI extends only to information the *government* creates or possesses, or that an entity creates or possesses *on behalf of* the government. In this example, licensees would not need to change their handling of the information, and an information sharing agreement would not be required.

The development of external stakeholder agreements with States will require interfacing with the appropriate State officials in order to facilitate information sharing with the range of State agencies with which the NRC will need to share CUI. For example, the sharing of CUI is essential to implementing an effective National Materials Program, as the 37 Agreement States regulate approximately 85 percent of all radioactive materials licensees. In addition, the NRC will share CUI with Agreement and non-Agreement States involved in nuclear power plant emergency preparedness, shipments of Category 1 and 2 quantities of radioactive material, or security-related activities. The staff has initiated planning, through the NRC's Agreement State and Liaison Programs, to engage the States on how best to implement the CUI Program.

---

[7] In 32 CFR 2002.16(a)(5)(ii), the CUI Rule states that if it is not feasible to enter into a formal agreement with a non-executive branch entity, but the agency's mission nonetheless requires it to disseminate CUI to that entity, the agency must communicate to the entity that it "strongly encourages" that CUI be handled in accordance with the CUI Rule. Existing laws, regulations and Government policies that govern CUI-Specified (see Enclosure), must be followed whether or not an Agreement is in place with the non-executive branch entity taking receipt of the sensitive information.

The staff recognizes that the CUI Rule could alter how information is shared between the agency and external parties, including licensees, applicants, Agreement and non-Agreement States, and others. The staff is committed to minimizing negative impacts to external stakeholders in the implementation of the CUI Program. To this end, the staff intends to work with stakeholders to understand information sharing needs and to explore options for reducing potential burdens. In recognition of the potential imposition of new information-security burdens from enhanced security requirements and standards for information technology systems, the staff is currently exploring technical solutions (e.g. virtual workspaces that will allow collaboration in a document without the need to download it) that could allow for secure file sharing and collaboration in a manner that does not require external stakeholders to modify their information systems. Additionally, the staff will benchmark with other regulatory agencies to leverage other agencies' experiences and practices. The staff will explore options for information sharing agreements so as to reduce unintended consequences that unnecessarily increase the burden on external stakeholders while also maintaining adequate protective measures for CUI.

Rulemaking

The staff is assessing how the agency will need to revise its regulations as a result of the transition to the CUI Program. OCIO will ensure that each office has considered, with guidance from the Office of the General Counsel (OGC), how to revise any regulations under each office's purview. Based on the results of the assessment, the cognizant office will develop a rulemaking in accordance with the Commission's direction for statutorily-directed rule in SRM for COMSECY-17-0002, "Rulemakings Mandated by Statute or Implementing U.S. Government Policy on Export Licensing Controls," dated February 28, 2017 (Agencywide Documents Access and Management System No. ML17059D045). The Commission approved the staff's recommendation that "rulemaking plans do not need to be prepared for rulemakings that are mandated by statute or implement U.S. Government policy on export licensing controls, and involve no discretion as to the content of the rule."

Thus far, the staff has not identified all instances for which rulemaking would be required to allow the NRC to implement the CUI Program; however, the staff has identified some cases for which revisions to regulations could be beneficial to facilitate CUI Program implementation. For example, 10 CFR 2.390, "Public Inspections, Exemptions, Requests for Withholding," currently provides specific marking instructions to submitters of documents who request that those documents be withheld from public disclosure. Those marking instructions do not align with the CUI marking requirements. Unless amended when the NRC implements the CUI Program, 10 CFR 2.390 will continue to direct submitters to apply non-CUI markings to sensitive unclassified documents that they submit to the NRC. If the NRC grants the request to withhold the information, the NRC staff would be required to re-mark those documents with CUI-compliant markings.

Outreach and Communication

In recognition of the possible impacts to internal and external stakeholders, the staff is developing a communication plan to engage stakeholders on CUI implementation strategies, assess impacts on current processes, and solicit potential external stakeholders' concerns and suggestions. For example, the staff may hold public meetings to discuss the CUI Rule or host an information table or sessions at the NRC's Regulatory Information Conference in future years. Additionally, the staff is developing a CUI Web page on the agency Intranet and public Website to provide an overview of CUI, frequently asked questions, and the status of NRC CUI Program implementation.

Coordination with Federal Agencies

Consistency with Federal partners will be particularly important in areas in which CUI information is shared. For example, data acquired and exchanged under the U.S. Department of Energy (DOE) program on accident-tolerant fuel that the NRC is reviewing for licensing is an area in which the NRC and the DOE will need to be fully aligned on the classification of the data. The staff will continue to work with NARA and other Federal agencies to identify best practices for implementing CUI requirements and for sharing CUI with non-Executive Branch entities.

RESOURCES:

Resources for CUI implementation are included in the FY 2018 President's Budget in the Operating Reactors, New Reactors, and Nuclear Materials Users Business Lines, under the Mission Support and Supervisors product line, and in the Corporate Support Business line under the Information Technology/Information Management Resources and Administrative Services product lines. In FY 2018, 3 FTE and $876K are included in the budget for the transition to CUI and the information management portion of the agency's SUNSI, SGI, CUI, and Classified Information Security Programs. The FY 2019 President's Budget includes 4 FTE and $576K for the same programs. Since the development of the FY 2018 and 2019 budgets, NARA has provided additional CUI implementation information that the staff used to inform its implementation plan. To effectively implement the new CUI program, additional resources will be needed beyond those budgeted in FY 2018 and FY 2019. Additional funding needs will be addressed during the FY 2018 and FY 2019 budget implementation process. Resources for FY 2020 and beyond will be addressed in the Planning, Budgeting, and Performance Management process.

CONCLUSION:

The staff is actively working to implement the CUI Rule and is currently developing an NRC CUI policy and revising MD 12.6. These documents will serve as the foundation of the Agency's CUI Program and will influence the content of other MDs and guidance documents. Additionally, the staff is developing a communication plan and strategies for engaging internal and external stakeholders. The CUI Program multi-project framework and implementation strategy identify activities required to be completed during the next 3.5 years in order to implement the CUI Program. The staff will inform the Commission of any policy or resource issues.

COORDINATION:

OGC has reviewed this paper and has no legal objection. The Office of the Chief Financial Officer has reviewed this paper for resource implications and has no objections.

/RA Dan Dorman Acting for/

Victor M. McCree
Executive Director
for Operations

Enclosure:
Background on Controlled Unclassified Information

SUBJECT: UPDATE ON DEVELOPMENT OF THE CONTROLLED UNCLASSIFIED INFORMATION PROGRAM DATED: March 8, 2018

SECY- 200900185-OCIO

ADAMS Accession Number: ML18065B107 ***via email**

OFFICE	OCIO/GEMS: PM	OCIO/GEMS: BC	OCIO/GEMS: D	OCIO: DCIO	NRO: DD/DEI*
NAME	SMroz	MJanney	JMoses	S. Flanders	R. Caldwell
DATE	02/23/18	03/06/18	02/23/18	02/23/18	02/26/18
OFFICE	NRR: D/DSS*	NSIR: DD*	NMSS: D/MSTR*	RES: D*	ADM: DD*
NAME	MGavrilas	JLubinski	KWilliams	M. Weber	M. Lombard
DATE	03/01/18	03/06/18	02/28/18	02/28/18	03/05/18
OFFICE	OE: DD*	OCHCO: DD*	OI: DD*	OIP: DD*	R-IV: DRA*
NAME	FPeduzzi	JGolder	SJefferson	DSkeen (GLanglie for)	S. Morris
DATE	02/27/18	02/26/18	02/28/18	02/27/18	02/26/18
OFFICE	OCFO: DCFO*	Tech Editor*	OGC*	OCIO: CIO	EDO
NAME	BFicks	KAzariah-Kribbs	JAdler	D. Nelson	V. McCree (DDOrman for)
DATE	02/23/18	02/26/18	03/06/18	03/06/18	03/ 08 /18

OFFICIAL RECORD COPY

Background on Controlled Unclassified Information

Controlled unclassified information (CUI)[1] is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable laws, regulations, and Governmentwide policies but is not classified under Executive Order 13526, "Classified National Security Information," dated December 29, 2009, or the Atomic Energy Act of 1954, as amended. CUI is a designation that is intended to standardize and simplify the way the executive branch handles unclassified information that requires safeguarding or dissemination controls. The U.S. Nuclear Regulatory Commission (NRC) CUI Program will replace existing agency programs such as For Official Use Only, Sensitive But Unclassified, Official Use Only, and Sensitive Unclassified Non-Safeguards Information. The CUI Program will also include within its scope the NRC's Safeguards Information (SGI) program, although the effects on the SGI program, as discussed below, should be less than for other types of NRC CUI. The CUI Program will address the current patchwork of more than 100 agency-specific policies throughout the executive branch, which have been found to lead to inconsistent marking and safeguarding as well as overly restrictive dissemination policies.

The CUI Rule identifies the National Archives and Records Administration[2] (NARA) as the Executive Agent to implement Executive Order 13556 and to oversee agency actions to ensure compliance with the Executive Order, the CUI Rule and the CUI Registry[3]. NARA's Information Security Oversight Office (ISOO) issued Title 32 of the *Code of Federal Regulations* (32 CFR) Part 2002, "Controlled Unclassified Information" (CUI Rule), to establish policy for agencies on designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI, self-inspection and oversight requirements, and other facets of the CUI Program. The rule applies to all executive branch agencies that designate or handle CUI and non-executive branch entities that manage CUI information on behalf of Federal agencies. Additionally, before sharing CUI with other non-executive branch entities, agencies must, whenever feasible, enter into agreements that require the non-executive branch entity to handle the information consistent with the CUI Rule.

The CUI Rule designates two general categories of CUI: (1) CUI Basic and (2) CUI Specified. CUI Basic refers to CUI for which law, regulation, or Governmentwide policy does not identify specific controls. For CUI Basic, the controls identified in the CUI Rule would govern the handling, protection, destruction, and dissemination of the information; that is, CUI Basic is the default set of standards for CUI. CUI Specified refers to CUI for which law, regulation, or Governmentwide policy does identify particular controls, either by requiring or permitting specific controls for that information. The CUI Rule does not alter those specified controls. Thus, for CUI Specified, agencies continue to apply the controls specified in existing law, regulation, or Governmentwide policy, and apply CUI Basic standards in areas where those authorities are silent. For example, a Federal law may specify how to handle certain sensitive information, but not specify how to destroy that information once it is no longer needed. If the information is CUI Specified—agencies would apply the handling controls specified in the Federal law, and would also apply the CUI Basic standards for its destruction. Two notable

[1] Executive Order 13556 "Controlled Unclassified Information," dated November 4, 2010, established the CUI Program.
[2] The NARA webpage (https://www.archives.gov/cui) includes comprehensive information on the CUI Program.
[3] The publicly available CUI Registry developed by NARA (https://www.archives.gov/cui/registry/category-list) is the online repository for all information, guidance, policy, and requirements on handling CUI, including everything issued by NARA on CUI. Among other information, the CUI Registry identifies all approved CUI categories and subcategories, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes guidance on handling procedures.

examples of CUI Basic and CUI Specified at the NRC are Security Related Information (SRI) and Safeguards Information (SGI), respectively. The CUI Rule would govern the control measures for SRI because no law, regulation, or governmentwide policy specifies particular controls for it. However, the NRC has established particular control requirements for SGI under 10 CFR Part 73, "Physical Protection of Plants and Materials". Even though SGI would be a form of CUI under the CUI Rule, any specific controls found in 10 CFR Part 73 would continue to apply to SGI.

Responsibilities

Executive branch departments and agencies continue to review the categories, subcategories, and markings in the CUI Registry that will be used to designate unclassified information for safeguarding and dissemination controls and can submit proposed changes to NARA for review and approval. NARA consults with affected agencies and non-governmental stakeholders to develop and issue directives that are necessary to implement the CUI Program. The implementation of agencies' CUI Programs will take place based on guidelines established by NARA, in consultation with the Office of Management and Budget, and departments and agencies.

Each executive branch department and agency is responsible for identifying a mechanism (i.e., office or individual(s)), responsible for administering the CUI Program. Agencies must also develop tailored CUI policies to meet agency-specific needs, and establish an internal oversight mechanism to promote consistent practices.

Agencies are responsible for ensuring that their personnel are properly trained in practices related to CUI.

Additional Information

NRC Transition to CUI

- Until directed by the NRC's CUI policy, guidance, and training, NRC employees and contractors must not use CUI markings or follow other requirements specific to CUI.

- If NRC employees or contractors receive CUI before the implementation of the CUI Program at the agency, they must follow current NRC guidance to protect sensitive information.

CUI Relationship to the Freedom of Information Act (FOIA) and Classified Information

- The CUI Program does not change NRC policy and practices in responding to a FOIA request. Marking and designating information as CUI does not preclude information from release under the FOIA or preclude it from otherwise being considered for public release. The staff must still review the information and apply FOIA exemptions appropriately.

- The CUI Program is separate from the Classified National Security Information program. While the programs may share similar language and some similar requirements, CUI Program requirements for designating, protecting, accessing, sharing, and decontrolling information, as well as the repercussions for misuse, differ from those for the classified information program.