INTELLIGENCE INSIGHTS

EXPERT INSIGHTS ON NATIONAL
SECURITY DEVELOPMENTS

OCTOBER 2021

Complex, Confusing, and Costly: Challenges Implementing the Government's Controlled Unclassified Information (CUI) Program

PRESENTED BY INSA'S SECURITY POLICY REFORM COUNCIL

SECURITY POLICY
REFORM COUNCIL

EXECUTIVE SUMMARY

Postmortem reviews of the September 11 attacks highlighted the need for the federal government to overcome a patchwork of agency-specific policies for controlling sensitive materials and share information more widely among federal, state, local, and private sector officials. The government established a program to define and protect Controlled Unclassified Information (CUI) by Executive Order in 2010, with detailed rules issued in 2017.

The new rules, however, are complex, confusing, and costly to implement, and they are applied inconsistently across agencies. CUI compliance will require U.S. Government (USG) agencies and contractors to invest enormous amounts in information technology systems and document control systems to govern access to more than 120 distinct categories of CUI that each require unique protections.

If the CUI Program is to succeed, it must set clear, uniform rules that contractors can implement consistently for clients across the federal government. The CUI Executive Agent must standardize practices across agencies and continue to address industry feedback on implementation challenges. Unless the Program is re-evaluated and reformed, it will have replaced the pre-9/11 system of ad hoc, agency-specific policies, procedures, and markings with a new system that has the same problems.

INTRODUCTION

Since the September 11 postmortem review highlighted the need for government agencies to share information more effectively,[1] the federal government has been developing a program to both protect and appropriately share information that requires safeguarding or dissemination controls but is not classified national security information. To promote secure information-sharing, the president ordered the establishment of a CUI program in a November 2010 executive order (E.O. 13556),[2] and detailed program rules were issued in 2017.[3]

Previously, this information had been protected though an unregulated assortment of document markings that differed across government agencies. Although the CUI Program was established to simplify and codify the patchwork of agency-specific policies for controlling sensitive materials, the new rules are complex, confusing, and costly to implement, and they are applied inconsistently across agencies. CUI compliance will require USG agencies and contractors to invest enormous amounts in information technology systems and document control systems to govern access to more than 120 distinct categories of CUI that each require unique protections. The Program is so complex, costly, and inconsistently implemented that in December 2020, then-Director of National Intelligence (DNI) John Ratcliffe formally requested that the president rescind the executive order establishing the program, asserting that the CUI Program was "vastly overcomplicated" and "unsustainable" with an estimated implementation cost of more than $1 billion in the Intelligence Community alone.[4]

Not surprisingly, government agencies themselves are having difficulty implementing CUI rules. On September 23, 2021 – 18 months after the Department of Defense (DOD) issued guidance on CUI implementation[5] – the DOD Acting Inspector General (IG) released a Management Advisory regarding the Department's "Ineffective Implementation of the Controlled Unclassified Information Program."[6] The IG states that continued use of outdated markings violates DOD guidance and risks the inadvertent release of sensitive information. The IG went on to "recommend that the Under Secretary of Defense for Intelligence and Security develop and implement an action plan, with milestones, to oversee CUI training within the DoD and the effective implementation of the DoD CUI Program by all DoD Components." The IG's memorandum highlights the difficulty of implementing the CUI program across a large enterprise and suggests that government agencies' ability to comply with CUI Program rules remains a long way off.

Because contractors provide wide-ranging support to virtually every federal agency, industry's proactive participation in the CUI Program is essential for its success. Federal partner firms have valuable insights into the challenges of CUI implementation and can articulate concerns regarding program requirements, effectiveness, feasibility, cost, and consistency of implementation across government. Industry has shared its concerns with the National Archives and Records Administration's (NARA) Information Security Oversight Office (ISOO), which oversees the CUI Program, through consultative mechanisms such as the National Industrial Security Program Policy Advisory Committee (NISPPAC).

INSA surveyed its member firms to identify concerns regarding the CUI Program and its implementation, soliciting insights regarding both perceived future problem areas and lessons learned from the limited Program implementation to date. This paper captures industry misgivings and offers concrete recommendations for improving the effectiveness of the CUI Program.

ISSUES AND AREAS OF CONCERN

METHODOLOGY

Over the last several years, INSA has tracked the development of the CUI Program and has sought the opinions, experiences, and concerns of its member firms, both large and small businesses. The questions asked included:

- Will the underlying objectives of the CUI Program – the protection of sensitive information in an efficient, uniform manner so it could be shared more easily in a secure manner – be met by the current approach?
- Do CUI requirements adequately reflect the experiences of, and potential impacts on, industry?
- Have the requirements and costs of implementing the CUI Program been adequately articulated for industry?
- Does the CUI Program's implementation reflect current and future business practices, information technology, social behaviors, network inter-dependencies, and availability of public information?

FINDINGS

INSA's survey revealed the following issues and areas of common concern with the evolving implementation of the CUI Program.

1. **CUI rules are more complex than the problem they are intended to solve.** The Program's current rules fail to simplify the "inefficient, confusing patchwork" of policies, procedures, and document markings that Executive Order 13556 was designed to reform. As of 2021, the CUI Program has identified 125 categories of CUI in 20 groupings.[7] Topics range from naval nuclear propulsion information regarding ship-borne nuclear reactors (CUI//NNPI), confidential federal grand jury information (CUI//JURY), and witness protection files (CUI//WIT) to patent applications (CUI//APP), archeological resources (CUI//ARCHR), national park system resources (CUI//NPSR), and railroad safety analysis records (CUI//RAIL). Each category has unique requirements for marking,[8] storage, access, dissemination,[9] destruction, staffing, record-keeping and reporting.

   One could argue that the CUI program at least defines and limits the number of sensitive information categories, which were previously completely unregulated. Nevertheless, the establishment of 125 distinct categories for CUI that each have unique handling requirements imposes a significant burden on the companies and agencies that have to track this data and regulate access to it.

2. **CUI adoption, requirements, and implementation rules differ across agencies.** Although CUI rules require all agencies to implement the program uniformly, in practice some agencies imposed their own implementation guidelines and oversight requirements. ISOO acknowledged these differences in an analysis of public comments on CUI rules, noting, "the rule does not prohibit agencies from promulgating agency-specific policies. Agencies are still able to set out agency policies and practices within their own documents and programs, and are, in fact, expected to promulgate CUI Program implementing policies within their agency to carry out the regulation's requirements."[10] This lack of consistency presents challenges and creates additional costs for firms supporting multiple USG agencies.

3. **The CUI Program office has not defined measures of effectiveness.** ISOO has not defined measures of effectiveness to determine whether and to what extent the CUI Program is achieving its objective to improve secure information-sharing. Given that the Program will impose significant costs and administrative burdens on industry (as well as government), it is important to know whether or not CUI measures are adding value so the Program can be periodically evaluated and improved. Without performance metrics, ISOO will be unable to assess the Program's impact, weigh the benefits against the costs incurred, or make adjustments to improve its execution.

4. **Industry adherence to CUI standards is being managed by already overworked government acquisition staffs.** Details regarding CUI designation, implementation, and management by contractors are left to the acquisition staffs of individual departments, agencies, and sub-agencies to define, which could create a new patchwork of practices that differ across contractors' multiple clients. Furthermore, acquisition personnel – who are not security experts – are already overstretched, and will be further taxed by new responsibilities to define and oversee complex information management and information security requirements.

5. **The CUI Program has a weak central management mechanism to resolve inconsistent requirements and implementation across government.** The executive order designated NARA as the CUI Executive Agent (CUI EA), which in turn delegated associated responsibilities to ISOO. As CUI EA, ISOO is charged with developing CUI guidance, overseeing implementation, and approving agencies' CUI policies to ensure their compliance with the rules.[11] The CUI EA is given some authorities to resolve interagency disputes regarding the designation of information as CUI.[12] However, the CUI EA is not empowered to resolve inconsistent agency practices for managing CUI; in fact, ISOO guidance encourages agencies to negotiate MOUs or interagency agreements with each other to address disparities and to "avoid duplicative and unnecessarily burdensome oversight actions" when overseeing contractors' handling of CUI.[13] Despite the CUI EA's formal role in overseeing CUI implementation across the government, ISOO has directed individual agencies to resolve inconsistent practices. Over time, the Program will inevitably be governed by a criss-crossing mélange of bilateral interagency agreements rather than a single set of rules applied uniformly across the government by the CUI EA.

6. **No uniform system exists for calculating or accounting for CUI implementation and compliance costs.** ISOO has not developed a methodology for determining the projected cost of implementing CUI in government or in the private sector. Individual agency acquisition elements are charged with managing the information technology, physical infrastructure, staffing, operations, maintenance, training and administrative costs of CUI implementation by industry. However, there is no commonly accepted way for contractors to account for, allocate, and recover CUI compliance costs, either on individual contracts, across contracts, or from contracts with multiple agencies.

7. **CUI rules do not clearly address ownership of proprietary information.** The government can designate as CUI any information that an outside entity, such as a federal contractor, creates or possesses for or on behalf of the Government.[14] When a company uses its proprietary data, approaches, technology, trade secrets, or software in the performance of work for the government, the government can therefore designate the entire, integrated work product (or components thereof) as CUI. Such a designation could limit the company from using its proprietary approach or intellectual property in its commercial business with non-government customers. To avoid such restrictions (and the costs and delays associated with litigating them), companies with significant commercial business may refrain from supporting government agencies or withhold their most innovative technologies from government customers.

8. **CUI compliance throughout complex supply chains will be difficult to ensure and verify.** Government contracts typically require CUI acquisition rules to be incorporated into subcontractor agreements. Prime contractors are therefore required to protect CUI throughout their supply chains. However, many large contractors have limited ability to ensure that their 3rd and 4th tier subcontractors have the training, expertise, and system controls to comply with CUI regulations. With an estimated 30 percent of the 220,000 companies in the Defense Department's supply chain alone handling CUI,[15] it will be extraordinarily difficult in practice to ensure and verify CUI compliance throughout the U.S. government's extensive network of vendors and subcontractors.

9. **CUI rules do not effectively protect legacy CUI information.** CUI rules (§2002.20.a.2) state clearly that all legacy (pre-CUI) markings should be discontinued, adding that any document marked with legacy designations – such as "Sensitive But Unclassified (SBU)," "For Official Use Only (FOUO)," and "Law Enforcement Sensitive (LES)" – do not qualify as CUI and therefore do not merit its protections.[16] This guidance inappropriately focuses on the age of document markings rather than the sensitivity of the information in those documents. As a result, although the CUI program is designed to protect sensitive information, this rule enables sensitive information to be disclosed simply because it is marked with out-of-date labels.

   Confusingly, given that old documents with out-of-date markings are no longer considered sensitive, CUI program rules (§2002.36.a) call for agencies to evaluate such materials and "individually remark legacy material that qualifies as CUI". This requirement acknowledges that information in documents with legacy markings may, in fact, still merit continued official protections. However, in the time it takes agencies to remark years' worth of legacy documents, the information they contain will have been handled without protections.

   Given the scale of the remarking effort, CUI rules (§2002.36.b) allow for waivers of the remarking requirement when the task is "excessively burdensome" (a standard that the rules do not define). This provision suggests that information that may, in fact, remain sensitive can go without CUI protections simply because the cost of evaluating and remarking documents is too high.[17]

   For contractors and government officials alike, this web of conflicting rules makes it difficult to know how to handle materials marked with legacy labels. If a contractor incorporates information marked FOUO into a document, the resulting product no longer merits protection. But if an agency later determines that the FOUO information merits CUI protections and labeling, the contractor will be in violation of CUI rules and subject to penalties.[18] Such contractual violations would require a review of document and network controls to re-establish compliance, a time-consuming and costly undertaking. Uncertainty about the impermanent status of information and the possibility that materials in a company's possession could unexpectedly be upgraded to CUI pose significant planning, management, contractual, and financial challenges for contractors.

IMPACTS

1. Despite the CUI Program's outreach and education, the absence of whole-of-government governance, precise implementation guidance, and centralized dispute resolution mechanisms will continue to limit its overall acceptance and adoption.
2. Without precise, uniform, and comprehensive implementation guidance and cost recovery options from the USG, industry may be unable to meet the CUI requirements in a cost-effective manner, potentially resulting in program failures and increased costs.
3. The impact of these program shortcomings will be especially high for companies that support multiple agencies with conflicting policies, requirements, acquisition systems, and compliance structures. Such companies will have to create a complex web of access controls to networks, documents, and facilities that complicates compliance and increases costs.
4. The need to configure complex personalized access controls on IT systems to meet CUI requirements may be prohibitive for smaller firms, potentially deterring innovative firms from working with the USG and reducing USG access to cutting-edge technologies.
5. Uncertainties regarding costs, compliance, and intellectual property protections may drive firms developing technologies with both government and commercial applications to focus on commercial markets instead of partnering with government agencies.

RECOMMENDATIONS

1 Reassess what really needs protection – and whether the CUI Program, as constituted, achieves that goal. ISOO should consider whether every USG agency or department needs complex CUI rules based on its unique mission needs, threat vectors, and existing safeguards. Data related to the location, character, or ownership of historic properties (CUI//HISTP), for example, may not merit the same protections as information related to the security of nuclear facilities and radioactive materials (CUI//SRI).[19] Focusing the CUI Program's attention and resources on information that requires significant protections would enhance the likelihood of success, reduce burdens on both government and industry, and free up financial and human resources. If changes are merited to strike an appropriate balance between information protections and transparency, reduce administrative burdens, or better allocate finite resources, ISOO should propose revisions to Program rules and, as necessary, recommend legislative changes to Congress.

2 Simplify the CUI program. Executive Order 13556 directs the establishment of an open and uniformly implemented program for managing unclassified information that requires special safeguards. It does not call for a complex new "classification" and "control" system with dozens of categories and sub-categories. ISOO should reassess the program's design and recommend to Administration policymakers new rules that would truly simplify the "inefficient, confusing patchwork" of policies, programs, and markings that existed previously. As it considers how to bring the CUI Program back to the EO's "first principles" of openness and uniformity of government-wide practice, ISOO should consider lessons learned from the government's prior experiences addressing over-classification and reducing barriers to information sharing.

3 **Clarify impact of CUI designation on proprietary information.** CUI designation of proprietary information is meant to prevent the government from releasing a company's intellectual property or trade secrets to its competitors or to the public. However, such designation could be interpreted as implying that even the originating company cannot use the data without government approval. CUI rules should clarify that the "Proprietary Manufacturer" CUI designation (CUI//SP-MFC) applies to any corporate proprietary information and imposes no restrictions on the organization that originally provided the information to the government.

4 **Evaluate the effectiveness of CUI controls in light of today's cyber threats.** The CUI Program, which was established by Executive Order in 2010, focuses heavily on the marking and control of individual documents. CUI Program rules – which go to great length to specify how hard copy documents should be protected, accompanied by cover sheets, reproduced, and transmitted securely by means including the U.S. Postal Service and facsimile[20] – constitute an industrial age approach to information management. Recent cyber advanced persistent threat (APT) attacks have by-passed marking-based controls and directly accessed both government and commercial IT systems. Given the complexity, interconnectivity, and vulnerability of modern IT systems, ISOO should reconsider whether a system predicated on the marking, handling, transmission, and control of individual "documents" is the best way forward.

5 **Evaluate CUI requirements in light of industry's supply chain structures.** Given the breadth of today's industrial supply chains, in which prime contractors engage a wide variety of subcontractors and vendors for specialized services, ISOO should work with industry to develop a more feasible approach to handling CUI across extended industrial networks. Such discussions should include acquisition officials from across the government, particularly the Defense Department, the Intelligence Community, and the General Services Administration (GSA), to ensure alignment between CUI rules and acquisition processes.

6 **Codify how CUI implementation costs will be calculated for industry bidding and compensation.** Effective contracting requires a consistent definition of how to estimate, bid and recover costs associated with CUI Program implementation. In particular, agencies must specify how CUI implementation costs can be accounted for across common projects and multiple agencies.

7 **Establish an ongoing mechanism for incorporating industry comments and recommendations.** An established forum for convening and eliciting industry representatives for the purpose of giving constructive feedback and recommendations for a responsive and cost-effective implementation of the CUI Program would be valuable. Such a mechanism could be hosted by the NISPPAC, a not-for-profit industry association, or a Federally Funded Research and Development Center (FFRDC).

8 **Revise CUI rules to clarify handling of legacy-marked materials.** To prevent the release of legacy-marked information that remains sensitive, CUI rules should be revised to direct the continued protection of such information unless it is explicitly reviewed and designated as suitable for public disclosure. To ensure that newly created documents citing legacy-marked materials are properly labeled with new CUI categories, revised CUI rules should direct that legacy-marked materials must be reviewed whenever they are referenced by, or incorporated into, subsequent documents.

CONCLUSION

The CUI Program's principal goal is to label sensitive but unclassified information clearly so it can be shared in a secure manner. However, the explosion of CUI categories, overly complex protection / handling guidelines, and a lack of strong centralized management authority undermine the program's effectiveness. At the same time, onerous implementation requirements burden government contractors with the need to implement multiple inconsistent information management and security practices – all while imposing consequences for failing to adhere to variable guidance or to protect information whose status as CUI can change without warning.

If the CUI Program is to succeed, it must set clear, uniform rules that contractors can implement consistently for clients across the federal government. The CUI EA must standardize practices across agencies and continue to solicit industry feedback on implementation challenges. Unless the Program is re-evaluated and reformed, it will have replaced the pre-9/11 system of ad hoc, agency-specific policies, procedures, and markings with a new system that has the same problems.

REFERENCES

[1] See, for example, Government Accountability Office, 9/11 Commission Report: Reorganization, Transformation, and Information Sharing, GAO-04-1033T, August 3, 2004. At https://www.gao.gov/products/gao-04-1033t.

[2] Executive Order 13556, 75 Fed. Reg. 216 (November 9, 2010). At https://www.govinfo.gov/content/pkg/FR-2010-11-09/pdf/2010-28360.pdf.

[3] CUI rules are codified at 32 CFR 2002. See Controlled Unclassified Information (CUI), 32 C.F.R. §2002 (2017). At https://www.govinfo.gov/content/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf.

[4] Director of National Intelligence John Ratcliffe, Memorandum to National Security Advisor Robert O'Brien, document ES-2020-01207, December 4, 2020. At https://fas.org/sgp/othergov/intel/ratcliffe-cui.pdf.

[5] "Controlled Unclassified Information (CUI)," DoD Instruction 5200.48, March 6, 2020. At https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520048p.PDF.

[6] Office of the Inspector General, Department of Defense, "Management Advisory Regarding the Continued Use of Unauthorized 'For Official Use Only' Markings and the Ineffective Implementation of the Controlled Unclassified Information Program," Report DODIG 2021-135, September 23, 2021. At https://www.dodig.mil/reports.html/Article/2789235/management-advisory-regarding-the-continued-use-of-unauthorized-for-official-us/.

[7] For the list of CUI groups and categories, see National Archives and Records Administration (NARA), "CUI Categories," web site. At https://www.archives.gov/cui/registry/category-list.

[8] For the list of CUI markings, see NARA, "CUI Markings," web site. At https://www.archives.gov/cui/registry/category-marking-list. For guidance on marking documents, see "Marking Controlled Unclassified Information," version 1.1, December 6, 2016. At https://www.archives.gov/files/cui/documents/20161206-cui-marking-handbook-v1-1-20190524.pdf.

[9] For the list of dissemination controls, see NARA, "CUI Registry: Limited Dissemination Controls," web site. At https://www.archives.gov/cui/registry/limited-dissemination.

[10] See 81 FR 63323 (September 14, 2016). At https://www.federalregister.gov/d/2016-21665/p-28.

[11] 32 C.F.R. §2002.8.a.4.

[120] 32 C.F.R. §§2002.50 – 2002.52.

[13] Information Security Oversight Office, "CUI Notice 2019-04: Oversight of the Controlled Unclassified Information (CUI) Program within Private Sector Entities," September 6, 2019, paras. 9-10. At https://www.archives.gov/files/cui/documents/20190906-cui-notice-2019-04-privatae-sector-entities.pdf. See also Information Security Oversight Office, "CUI Notice 2020-04: Assessing Security Requirements for CUI in Non-Federal Information Systems, June 16, 2020, para 10. At https://www.archives.gov/files/cui/documents/20200616-cui-notice-2020-04-assessing-security-requirements-in-non-fed-info-systems.pdf.

[14] 32 C.F.R. §2002.4(h).

[15] Chris Cornillie, "Defense Industry Waits on Costly Trump-Era Cyber Rule Update," Bloomberg Law, August 11, 2021. At https://news.bloomberglaw.com/privacy-and-data-security/defense-industry-awaits-update-on-costly-trump-era-cyber-rule.

[16] 32 C.F.R. §2002.20.

[17] 32 C.F.R. §§2002.36 – 2002.38.

[18] In an analysis of the public comments received on the proposed CUI rules, ISOO notes that companies could be penalized if they possess CUI that is unmarked or improperly marked, even if they are not at fault. Specifically commenting on provisions regarding the marking of legacy controlled information, ISOO writes, "The regulation does contemplate the possibility that some CUI may be unmarked or marked improperly. In such cases, agencies and non-executive branch agencies would still be subject to that CUI's governing law, regulation, or Government-wide policy's requirements, including any penalties or sanctions for not handling it properly in accord with those authorities or the connected CUI Program requirements." See 81 FR 63323 (September 14, 2016). At https://www.federalregister.gov/d/2016-21665/p-88.

[19] The CUI category of Historic Properties (CUI//HISTP) is described as information "Related to the location, character, or ownership of historic property." See NARA, "CUI Category: Historic Properties," web site. At https://www.archives.gov/cui/registry/category-detail/historic-properties. The CUI Category of Nuclear Security-Related Information (CUI//SRI) is described as "information that could be useful, or could reasonably be expected to be useful, to a terrorist in a potential attack … including the exact location and quantities of radioactive material, certain detailed design drawings, information on nearby facilities, emergency planning information, and certain assessments of vulnerability and safety analyses." See NARA, "CUI Category: Nuclear Security-Related Information," web site. At https://www.archives.gov/cui/registry/category-detail/nuclear-security-related-info.html.

[20] See, for example, 32 C.F.R. §2002.14(d) regarding shipping, §2002.14(e)(2) regarding copying and faxing, and §2002.32 regarding cover sheets.

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

ACKNOWLEDGEMENTS

INSA expresses its appreciation to the INSA members and staff who contributed their time, expertise, and resources to this piece.

MEMBERS

Charlie Allen, *SPRC Chair*

Kathy Pherson, *SPRC Vice Chair*

Tony Spadaro

Bryan Denson

John Ellingson

Jeremy Erb

Cathe Kaohi

Charlie Sowell

Michael Steinbuch

Susan Steinke

Katie Timmons

Greg Torres

INSA STAFF

Suzanne Wilson Heckenberg, *President*

John Doyon, *Executive Vice President*

Larry Hanauer, *Vice President for Policy*

Peggy O'Connor, *Director of Communications and Policy*

Britany Dowd, *Marketing and Communications Assistant*

Nicholas Damianos, *Intern*

ABOUT INSA

The Intelligence and National Security Alliance (INSA) is a nonpartisan, nonprofit forum for advancing intelligence and national security priorities through public-private partnerships. INSA's government and private sector members collaborate to make government more effective and efficient through the application of industry expertise and commercial best practices. INSA's 160+ member organizations are leaders in intelligence collection and analysis, data analytics, management consulting, technology development, cybersecurity, homeland security, and national security law, and its 4,000 individual and associate members include leaders, senior executives, and intelligence experts in government, industry, and academia.

ABOUT INSA'S SECURITY POLICY REFORM COUNCIL

INSA's Security Policy Reform Council seeks to transform the paradigms that govern the design and execution of security policy and programs and to serve as a thought leader on security issues. The Council works with industry, academic and government stakeholders to identify and mitigate security challenges, develop security solutions, advocate for reforms to enhance the effectiveness of security policy and programs, and enhance industry's ability to support and protect national security.