INTELLIGENCE AND
NATIONAL SECURITY ALLIANCE

POSITION PAPER

January 2020

Getting it Right:

Establishing Uniform Policies for Controlled Unclassified Information

Prepared by
THE INSA SECURITY POLICY REFORM COUNCIL

SECURITY POLICY
REFORM COUNCIL

EXECUTIVE SUMMARY

Leading federal contractors are warning that without specific, uniform, and comprehensive implementation and cost recovery options, proposed acquisition rule changes to implement the federal Controlled Unclassified Information (CUI) program will result in increased costs and program failure. Federal Acquisition Regulation (FAR) clauses are in the process of being finalized over the coming 12-18 months. After that point, departments and agencies will be required to adopt new policies and procedures based on forthcoming implementation guidance. During this implementation period, the National Archives' Information Security Oversight Office (ISOO), which administers the CUI program, must ensure the feasibility of provisions addressing nine different challenges: **(1) agency priorities and resources to implement new CUI rules, (2) standards for access to CUI, (3) implementation costs, (4) consistency, (5) proprietary information, (6) supply chain, (7) legacy data, (8) compliance management,** and **(9) acceptance and adoption.**

BACKGROUND

According to the National Archives, Controlled Unclassified Information (CUI) is "information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended."[1] The handling of this information is complicated by the existence of 124 categories of CUI within 20 distinct organizational groups.[2] Although the Archives is developing consolidated CUI guidance for all government agencies, more than 100 executive branch departments and agencies maintain their own practices for CUI. As a result, a patchwork of rules dictates how this information must be categorized, stored, handled, disseminated, and destroyed.[3] Furthermore, as ISOO has acknowledged, individual agencies are struggling to implement the Archives' guidance, making it likely that the new rules will be inconsistently interpreted and applied.

Federal contractors typically support multiple government agencies and must therefore ensure their internal computer systems and their document handling and storage practices comply with this broad range of sometimes conflicting rules

1 See National Archives, "About Controlled Unclassified Information (CUI)," web site, updated August 1, 2019. At https://www.archives.gov/cui/about.

2 National Archives, "CUI Categories," web site, updated February 11, 2019. At https://www.archives.gov/cui/registry/category-list.

3 See National Archives, "CUI History," web site, updated August 6, 2019. At https://www.archives.gov/cui/cui-history.

and procedures. Such compliance measures are costly; they require complex standard operating procedures, carefully calibrated data access policies, multiple program managers, and, in many cases, additional hardware and software to oversee implementation. ISOO must ensure that the new CUI rules facilitate contractors' handling of multiple categories of CUI so these companies can successfully – and cost-effectively – support government missions.

CHALLENGES

To ensure that contractors can effectively support government agencies and execute their contracts, new CUI rules must address the following nine key challenges:

AGENCIES LACK RESOURCES AND INCENTIVES TO IMPLEMENT NEW CUI RULES

The implementation of new CUI rules is not a priority for most agencies, and few have allocated sufficient resources to implement them. ISOO acknowledged as much in its FY2018 Report to the President, writing, "Many agencies are struggling to issue their CUI implementing regulations, submit CUI budget proposals to OMB, implement the program's marking requirements, and staff their agency's CUI Program sufficiently. Solutions to these challenges will require senior agency leadership to prioritize implementing the CUI Program…ISOO assesses that agencies will not be able to fully implement the CUI Program without dedicated funds and sufficient levels of full-time staff."[4]

ABSENCE OF STANDARDS FOR ACCESS TO CUI

In the realm of classified information, personnel who pass thorough background investigations are granted security clearances with access to specific categories of information. The investigations and tiered levels of access (e.g., a Secret vs. a Top Secret clearance), which are recognized across government and industry, afford greater protection to more sensitive information.

However, no such system exists to govern access to CUI and its 124 sub-categories of information. Most of the government agencies and departments promulgating CUI depend upon Public Trust Eligibility standards – which all individuals working at government facilities must meet – to determine access to CUI information and to the facilities and systems that contain, store, and transmit CUI data. However, no uniform whole-of-government standards exist to assess whether and to what extent someone with a Public Trust Eligibility should be permitted to access some or all categories of CUI data.

Since there are no standards governing access to CUI, agencies are not required to grant an individual access to their own CUI simply because another agency previously did so. This lack of reciprocal access makes it difficult for contractor personnel to support multiple agencies that work with CUI. Before granting an individual access to their own CUI data, agencies may choose to conduct their own duplicative Public Trust Eligibility background check and suitability investigation, which increases costs to the government and causes delays in contract execution.

LACK OF CLARITY REGARDING IMPLEMENTATION AND COMPLIANCE COSTS

The cost for industry to implement and comply with new CUI requirements remains an open question. It is unclear whether such costs will be recoverable under contracts as either direct or indirect expenses. Additional and enhanced CUI requirements will increase overhead costs for contractors, which will inevitably result in higher contract prices for government. This will be especially true for programs designated critical and subject to "Advanced Persistent Threats (APT)," which will require enhanced contractor personnel vetting, access control, and training systems. New rules must specify how implementation and compliance costs will be allocated across agencies and individual contracts, specifically where a company's underlying CUI infrastructure may be shared across the firm.

LACK OF CONSISTENCY IN CUI IMPLEMENTATION

CUI data encompasses 124 categories of information within 20 distinct organizational groups. More than 100 executive branch departments and agencies maintain their own practices for handling CUI, resulting in a patchwork of rules for handling these myriad categories of data. Current internal government audits show that consistent CUI implementation guidance and program controls are absent both within and across individual contracting entities. With the application of CUI implementation guidance ultimately in the hands of individual federal contracting entities that are devoting different levels of resources to the task, differences in CUI implementation will be inevitable and problematic.

[4] National Archives Information Security and Oversight Office, 2018 Report to the President, August 16, 2019, p. 1. At https://www.archives.gov/files/isoo/images/2018-isoo-annual-report.pdf.

Many contracts will involve inconsistencies that create problems for contractors. Examples include:

A. When one federal entity declares certain information to be controlled while other entities do not, contractors will have to segregate and secure the data, thereby hindering access to the same data by experts working on other government agencies' contracts.

B. When an agency imposes controls on information that already exists in the commercial sector, firms must incur costs to protect data that already exists, unprotected, elsewhere.

OWNERSHIP OF PROPRIETARY INFORMATION

When contractors perform work for government clients, they draw on a wide range of information, technology, and methodologies that they consider proprietary intellectual property. When applied to sensitive government data or used to yield sensitive analytic conclusions, the government may consider contractors' tools and methodologies themselves to be sensitive. This dynamic raises a number of concerns about how contractors can protect their own data and intellectual property.

For example, it is unclear whether a federal agency may have the right to designate as CUI a contractor's proprietary information, design data, process details or other intellectual property if it was used in the preparation of a deliverable to the government. The mere concern that proprietary tools and information could become off-limits to non-government or foreign clients may make contractors reluctant to provide such insights to government clients.

SUPPLY CHAIN: LACK OF CLARITY ON SHARING CUI WITH SUBCONTRACTORS

A major focus of the government's CUI effort has been to protect controlled information throughout the supply chain, especially in contracting for the Department of Defense. CUI protections are expected to flow down to all subcontractors and vendors.

Several supply chain concerns and their potential resolution have yet to be adequately identified. For example, it is unclear how contractors are to protect CUI when securing components of CUI-designated systems from foreign suppliers. Additionally, many large-scale integrators may not know (or be able to identify) subcontractors below the first or second tier, making it difficult to prevent the dissemination of CUI-designated information to organizations that need such data to design component parts or software.

RECATEGORIZING LEGACY CUI INFORMATION

The CUI program is intended to reduce the number and proliferation of controlled data categories, marking, and handling requirements. The National Archives' current plan focuses on CUI designations and markings for future data, with no stated requirement to re-mark legacy categories of controlled data. If the current 124 categories of legacy controlled data will coexist with new data markings, the result will be more categories, not fewer, of controlled data, requirements, and complexity.

UNDEFINED STATUTORY AUTHORITIES, RULES, AND MECHANISMS REGARDING COMPLIANCE MANAGEMENT

Compliance concerns include: (a) responsibility for audit / control of CUI requirements, compliance, and enforcement; (b) dispute resolution mechanisms for CUI conflicts between (or within) individual federal entities; and (c) mechanisms to compel CUI compliance (as there are, under Title 18) other than contract termination.

Contracting entities may require contractors to have effective CUI control regimes in place. However, the specific elements, actions, and processes that qualify as an "effective" regime are largely left to the contractor to define. This creates the risk that a diligent and well-intended CUI control regime may be acceptable to one agency but not to others.

CONFUSION WILL CAUSE SLOW AND INCONSISTENT ADOPTION OF NEW RULES

Individual Departmental and Agency prerogatives will affect implementation of CUI rules and regulations. Despite the National Archives' outreach and education, the absence of whole-of-government governance, uniform standards for access, specific implementation guidance, and dispute resolution mechanisms will continue to limit overall acceptance and adoption.

CONCLUSION

ISOO must address these issues if the CUI regime is to be implemented effectively and consistently across government without hindering industry's ability to execute contracts in a cost-effective and efficient manner. Without specific, uniform, and comprehensive implementation guidance and cost recovery options from ISOO, industry may be unable to meet the intent of the requirements without significant (and time-consuming) additional investments, resulting in program delays and increased costs right from the start. The impact of these concerns will be especially high for small firms that cannot afford large-scale infrastructure investments and for companies that support multiple departments and agencies with conflicting policies, requirements, and compliance activities.

ABOUT INSA

The Intelligence and National Security Alliance (INSA) is a nonpartisan, nonprofit trade association dedicated to advancing collaborative, public-private approaches to intelligence and national security priorities. Through the application of industry expertise, leading-edge academic research and commercial best practices, INSA seeks to make the Intelligence Community more effective and efficient. Our 160+ member organizations and its 4,000+ individual and associate members include senior executives and intelligence experts in the public, private and academic sectors.

ABOUT THE INSA 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 and government stakeholders to identify and mitigate security challenges, develop security solutions, and advocate for security reforms to enhance industry's ability to support and protect national security.

ACKNOWLEDGEMENTS

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

INSA MEMBERS

Tony Spadaro, *Spadaro & Associates*

Melissa Clasen, *Eagle Ray*

J. Bryan Denson, *TransUnion*

Jeremy Erb, *Deloitte*

Daryl Goods, *Boeing*

Chris Hale, *Raytheon*

Mike King, *Northrup Grumman*

Steve Kipp, *L3 Technologies*

Mitch Lawrence, *Lawrence Solutions LLC*

Adam Lurie, *Convergent Solutions, Inc.*

Kathy Pherson, *Pherson Associates*

Charlie Sowell, *iWorks*

INSA STAFF

Suzanne Wilson Heckenberg, *President*

Chuck Alsup, *Former President*

Larry Hanauer, *Vice President for Policy*

Peggy O'Connor, *Policy & Communications Director*

Caroline Henry, *Marketing & Communications Assistant*

Jacqueline Schultz, *Intern*

Tyler Spyrison, *Intern*

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

Building a Stronger Intelligence Community

(703) 224-4672 | www.INSAonline.org