DTAG Working Group: Competing USG Requirements (Task #4)

January 16, 2014

Table of Contents

Working Group Members

Andrea Dynes, General Dynamics Corporation *(team leaders)*
Krista Larsen, FLIR Systems, Inc.

Dennis Burnett, Dennis J. Burnett, LLC
Dava Casoni, University of Southern California
Steve Cope, Avion Solutions, Inc.
Michael Cormaney, Luks Cormaney LLP
Barbara Dudas, Northrop Grumman
Christine McGinn, InterGlobal Trade Consulting, Inc.
Mike Miller, University of Central Florida
Dale Rill, Honeywell

Assignment

Initially, the DTAG working group #4 was tasked to conduct a "[s]urvey of industry on how they reconcile potentially competing requirements placed upon them by the USG in terms of protection of controlled unclassified information, including export controlled data." This tasking was further clarified to "[r]eview how various USG

agencies define controlled unclassified information (CUI), including export controlled technical data, and critical program information (CPI). Review the statutory, regulatory and other bases (e.g., policy or directive) for agency control. Assess how USG agencies impose potentially competing requirements on industry for protecting CUI and CPI."

In the conduct of this assignment, the DTAG researched the statutory, regulatory and agency guidance related to the identification, control and dissemination of CUI by several different U.S. Government agencies, studied the history of U.S. Government efforts to impose uniformity on the identification and control of CUI and CPI, interviewed several government experts, and polled colleagues to compile real-world industry experiences.

Overview of CUI and Related Designators

History of CUI

The 9/11 Commission Report and Subsequent Acts and Reports

The efforts to consolidate and standardize CUI are relatively recent USG actions, set into motion by *The 9/11 Commission Report,*[1] which highlighted poor interagency collaboration as contributing to the failure of the USG to make connections between the various intelligence pieces that led up to the attacks on September 11, 2001: "Information was not shared…Analysis was not pooled…Action officers should have drawn on all available knowledge in the government. The management should have ensured that information was shared and duties were clearly assigned across agencies…" To usher in a new era of interagency collaboration, the *Homeland Security Act of 2002*[2] created a cabinet-level Department of Homeland Security (DHS) to serve as a singular intelligence sharing entity, and tasked the President to "identify and safeguard homeland security information that is sensitive but unclassified" (SBU). Over the next two years, the newly-formed DHS[3] attempted to provide standardized definitions for SBU, but received overwhelming requests from the public for opportunities to contribute, and concerns from the scientific community that the results of their research could be adversely affected.[4] Finally, in May 2004, DHS issued a brief, 13-page Management Directive for the *SAFEGUARDING SENSITIVE BUT UNCLASSIFIED (FOR OFFICIAL USE ONLY) INFORMATION*[5] that did not attempt to define SBU, instead provided definitions for a handful of other similar terms, including For Official Use Only (FOUO), Protected Critical Infrastructure Information (PCII), [6] and Sensitive Security Information (SSI), [7] and was largely devoted to providing detailed information on the correct marking and transmission of FOUO information. Absent a definition for SBU, the next most relevant term was FOUO, defined as "unclassified information of a sensitive nature, not

---

[1] Available at: http://www.9-11commission.gov/report/911Report.pdf, released July 22, 2004.

[2] As required by P.L. 107–296, on the web at http://www.gpo.gov/fdsys/pkg/PLAW-107publ296/pdf/PLAW-107publ296.pdf.

[3] This task was delegated to the DHS by *Executive Order 13311*, on the web at http://www.gpo.gov/fdsys/pkg/FR-2003-07-31/pdf/03-19675.pdf.

[4] Seventy-five public groups wrote to DHS requesting public input on SBU in *"Sensitive But Unclassified" and Other Federal Security Controls on Scientific and Technical Information: History and Current Controversy*, updated February 20, 2004, on the web at https://www.fas.org/sgp/crs/RL31845.pdf.

[5] Abbreviated *MD 11042.1*, this directive is on the web at: http://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_110421_safeguarding_sensitive_but_unclassified_information.pdf.

[6] Also defined in 6 U.S.C. 131(3) Section 212(3) of the Homeland Security Act.

[7] Also defined in 49 C.F.R. Part 1520.

otherwise categorized by statute or regulation." This definition, if adopted for SBU, would have excluded export controlled information (e.g., ITAR-controlled information).

Despite similar recommendations to improve interagency data dissemination from additional reports,[8] by 2004, little progress had been made to actualize the information sharing initiatives and communication between agencies. Aforementioned public concerns regarding an overly-restrictive definition of SBU combined with little direction on the procedural aspects of interagency sharing were likely contributors to the slow start.

The Intelligence Reform and Terrorism Prevention Act of 2004 and Presidential Actions

The first tangible shift towards interagency transparency was established by the 108th Congress in its *INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004* ("IRTPA"),[9] which required the president to "…issue guidelines for acquiring, accessing, sharing, and using information, including guidelines to ensure that information is provided in its most shareable form…", and even included provisions for international sharing. To comply, President Bush issued both an Executive Order[10] and Guidelines[11] in 2005 to promote a culture of "sharing of Sensitive But Unclassified (SBU) information, including homeland security information, law enforcement information, and terrorism information" as well as providing for "procedures and standards for designating, marking, and handling SBU." Relevant to SBU, Guideline # 3 required that a process for the standardization of SBU be submitted for Presidential approval within 1 year, to be led by the Director of National Intelligence (DNI) and coordinated by the designated Program Manager responsible for information sharing across the Federal Government (PM-ISE), and 11 months later in November 2006 the Information Sharing Environment (ISE) Implementation Plan was released.[12]

The ISE Implementation Plan was ambitious in its provisions for deploying and operating the ISE. However, the Plan identified that its major obstacle was still the variety of SBU "types" in use by differing government agencies. It stated, "Absent an overarching, cross-community policy for terrorism information access and sharing, individual policies evolved to meet the needs of Federal departments and agencies shaped by their respective statutory authorities and responsibilities. The result is a body of overlapping or independent policy regimes, inconsistent procedures for handling SBU information, and multiple forums at the Federal level, for [State, local and tribal], and private sector organizations." The Plan reinforced this observation by citing a GAO Report[13] issued earlier that same year on the challenges of information sharing, which discovered that Federal agencies use at least 56 different sensitive but unclassified designations (16 of which belong to one agency) to protect sensitive information. This same GAO Report concluded that "the growing and non-standardized inventory of SBU designations and markings is a serious impediment to information sharing among agencies, between levels of

---

[8] These additional reports include: *Efforts to Improve Information Sharing Need to Be Strengthened,* August 2003, on the web at http://www.fas.org/sgp/gao/infosharing.pdf; *Establishing Effective Information Sharing with Infrastructure Sectors*, April 2004, on the web at http://www.fas.org/sgp/gao/gao-04-699t.pdf; and *MANAGING SENSITIVE INFORMATION, Departments of Energy and Defense Policies and Oversight Could Be Improved*, March 2006, on the web at http://www.fas.org/sgp/gao/sensitive.pdf.

[9] Available at: http://www.gpo.gov/fdsys/pkg/PLAW-108publ458/pdf/PLAW-108publ458.pdf.

[10] Executive Order 13388—*Further Strengthening the Sharing of Terrorism Information to Protect Americans*, on the web at http://www.gpo.gov/fdsys/pkg/WCPD-2005-10-31/pdf/WCPD-2005-10-31-Pg1592.pdf.

[11] *Memorandum on Guidelines and Requirements in Support of the Information Sharing Environment*, 41 WEEKLY COMP. PRES. DOC. 1874 (Dec. 16, 2005), on the web at: http://www.ise.gov/sites/default/files/Memo_on_Guidelines_and_Rqmts_in_Support_of_the_ISE.pdf.

[12] Available at: http://ise.gov/sites/default/files/ise-impplan-200611_0.pdf.

[13] According to GAO report (GAO-06-385) *Information Sharing: The Federal Government Needs to Establish Policies and Processes For Sharing Terrorism-Related and Sensitive But Unclassified (SBU) Information* (GAO: Washington, DC, 2006).

government, and, as appropriate, with the private sector. As with the DHS Management Directive, the ISE Implementation Plan also avoided defining SBU, instead introducing an early definition of another term, CUI:

> As used in this plan, Controlled Unclassified Information (CUI) is defined as categories of unclassified information that require controls that protect it from public release, both to safeguard the civil liberties and legal rights of U.S. citizens, and to deny information advantage to those who threaten the security of the nation.

Introduction of CUI

Nearly two years after the release of the ISE Implementation Plan, in May of 2008, President Bush signed a *Memorandum on the Designation and Sharing of CUI*,[14] formally adopting "CUI" as the single designator for all previously-SBU information:

> "Controlled Unclassified Information" is a categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is (i) pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government, and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. Henceforth, the designation CUI replaces "Sensitive But Unclassified" (SBU).

This definition of CUI, at part (ii), was designed to overlap with information that "under law or policy requires protection from unauthorized disclosure." The Memorandum established as Executive Agent the National Archives and Records Administration (NARA), tasked with overseeing CUI (previously presumed to be under the Program Manager, Information Sharing Environment) and also provides a "CUI Framework" to "facilitate the sharing of terrorism-related information among federal, State, local, tribal, private sector, and foreign partner entities." This Memorandum is also the first written acknowledgment of the "private sector" as a partner of the USG in its efforts to manage CUI. The Memorandum proposes two levels of CUI sensitivity (Controlled and Controlled Enhanced) and three document markings for CUI, and prohibits additional marking, safeguarding, or dissemination requirements or any creation of CUI categories or rules outside of the CUI Framework. The Executive Agent was to develop CUI policy standards and then monitor compliance with its CUI policy, standards, and markings. In keeping with the definition, part (ii), CUI designation was reserved only for that information required to be protected by statute, regulations, policy, or other guidance, and the Executive Agent was empowered to validate all CUI claims: "[D]etermination should be based on mission requirements, business prudence, legal privilege, the protection of personal or commercial rights, safety, or security. Such department or agency directives, regulations, or guidance shall be provided to the Executive Agent for review." The memo also established a CUI Council, as a sub-committee of the Information Sharing Council (ISC), to function as an interagency steering committee for CUI activities.[15]

Standardization of CUI

Continuing the previous efforts to resolve and consolidate SBU/CUI conflicts, 2009-2011 saw considerable effort towards standardization of CUI. In 2009, President Obama issued a Memorandum[16] directing the formation of a task force to generate recommendations to reform the current practice where "…each agency has implemented its

---

[14] Available at: http://www.archives.gov/cui/documents/2008-WH-memo-on-designation-and-sharing-of-cui.pdf.

[15] The CUI Council was later merged into the Information Sharing and Access Interagency Policy Committee, co-chaired by the National Security Staff's Senior Director for Information Sharing Policy and the PM-ISE. Source: http://www.archives.gov/cui/chronology.html.

[16] *Memorandum on Classified Information and Controlled Unclassified Information*, May 27, 2009, available at: http://www.archives.gov/cui/documents/2009-WH-memo-on-classified-info-and-cui.pdf

own protections for categorizing and handling SBU" and thus "there are more than 107 unique markings and over 130 different labeling or handling processes and procedures for SBU information."

The recommendations of this task force are found in the *Report and Recommendations of the Presidential Task Force on Controlled Unclassified Information*[17] which found several deficiencies in the current management of SBU/CUI. Of the concerns raised by the task force, these three likely created the most confusion for industry holders of USG CUI:

1. The Executive Branch performance suffers from interagency inconsistency in SBU policies, uncertainty in interagency settings as to exactly what policies apply, and inconsistent application of similar policies across agencies,
2. The absence of effective training, oversight, and accountability at many agencies results in a tendency to over-protect information as SBU, thus greatly diminishing government transparency, and
3. Markings are sometimes misunderstood as providing an independent basis for withholding documents from the public, Congress, or the courts, which in turn can undermine transparency, as well as public trust in government.

The Task Force Report offered recommendations to address each of these concerns:

1. A singular definition for CUI: as "All unclassified information for which, pursuant to statute, regulation, or departmental or agency policy, there is a compelling requirement for safeguarding and/or dissemination controls."
2. A single agency (the Executive Agent) to establish standard markings and guidance.
3. Clarification that CUI marking has no bearing on whether a record is releasable under FOIA.

Following on the findings and recommendation of the Task Force Report, Executive Order (EO) 13556[18] was signed November 4, 2010, reinforcing what prior documents had already concluded, that "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."

President Obama's EO 13556 also mandated a 180-day review of all categories, subcategories, and markings used to identify controlled information and submit to the Executive Agent a catalogue of proposed categories and subcategories of CUI and proposed associated markings for information designated, including the basis in law, regulation, or Government-wide policy for safeguarding or dissemination controls (just as required by Bush's May 2008, Memorandum, which was rescinded by this EO). The EO directed the creation of a public registry for authorized CUI categories, subcategories, markings, safeguarding, dissemination and decontrol procedures, and empowered the Executive Agent to review and ensure uniform application, resolve conflicts, and issue directives to implement the Order.

In 2011, after compiling and processing all the inputs received from the 180-day review, the Executive Agent completed three major tasks necessary for the move toward a consolidated understanding of CUI: it (1) issued its

[17] Available at: http://www.archives.gov/cui/documents/2009-presidential-task-force-report-and-recommendations.pdf.

[18] Available at: http://www.gpo.gov/fdsys/pkg/FR-2010-11-09/pdf/2010-28360.pdf

Initial Implementation Guidance for Executive Order 13556[19], (2) published the CUI registry on its website, and (3) submitted its first annual report to the President.[20]

The DoD adopted the CUI changes piecemeal. In 2012, the DOD issued an agency manual on Controlled Unclassified Information (CUI)[21] in order to "implement policy, assign responsibilities, and provide procedures for the designation, marking, protection, and dissemination of CUI and classified information, including information categorized as collateral, sensitive compartmented information (SCI), and Special Access Program" but delayed incorporating the CUI program established by Executive Order 13556 for one year, issuing an update to its Manual on March 19, 2013 to include these mandates.

Expected Future CUI Activities

In accordance with the Executive Orders, Memoranda, and Task Force Report, it is expected that the USG will continue to make progress on its efforts to define CUI and established common standards for its safeguarding and dissemination. The CUI Framework dictates that the Information Sharing Environment agencies complete implementation in 2013, with all non-excepted agencies completing implementation by May 2015.

CUI-"Like" Controls

The DTAG researched over a dozen USG agencies and offices for possible “CUI-Like” definitions and controls, including export controlled information. The group also examined relevant statutes, regulations and other USG policies or directives. The research revealed over 40 CUI-Like terms, which potentially overlap with export-controlled information (including information regulated under the ITAR). **See** attached “CUI & CPI Research Chart.”

In addition to the CUI processes overseen by the Executive Agent, CUI-"Like" controls are placed upon industry from various government agencies. Examples of these requirements, which follow, were brought to the attention of the DTAG because they contain many of the elements already associated with CUI (such as marking and/or safeguarding requirements), but use different nomenclature to describe the "CUI-Like" information.

DoD/DSS Controls on Cleared Contractor Information Systems

The Defense Security Service (DSS) has claimed oversight of certain unclassified information. Specifically, in 2010, it issued an Industrial Security Letter (ISL)[22] stating, "the NISPOM requires contractors to promptly report to the Federal Bureau of Investigation (FBI) (with a copy to DSS) information coming to the contractor's attention concerning 'actual, probable or possible espionage, sabotage, terrorism, or subversive activities' at any of the contractor’s locations … The NISPOM imposes this reporting obligation because the hostile acts … are… so serious that when they are directed against any of a contractor’s locations, they can pose a threat to classified information and to the security of the entire contractor."

---

[19] Controlled Unclassified Information (CUI) Office Notice 2011-01: Initial Implementation Guidance for Executive Order 13556, June 9, 2011, available at http://www.archives.gov/cui/documents/2011-cuio-notice-2011-01-initial-guidance.pdf.

[20] http://www.archives.gov/cui/reports/report-2011.pdf

[21] DoD Manual 5200.01, February 24, 2012, available at: http://www.dtic.mil/whs/directives/corres/pdf/520001_vol4.pdf

[22] ISL 2010-02, Reporting Requirements for Cyber Intrusions (NISPOM 1-301), February 22, 2010, available at: http://www.dss.mil/documents/pressroom/Rescinded%206-13-2013%20-%20ISL_2010_02.pdf

Subsequent to this letter, section 941 of the National Defense Authorization Act for Fiscal Year 2013 (NDAA 2013)[23] authorized the Secretary of Defense to establish procedures that require cleared contractors to report to the DoD designate agency when a network or information system is successfully penetrated, including provisions to surrender compromised equipment for forensic analysis to determine the level of exfiltration.

In May of 2013, DSS rescinded its 2010 ISL and replaced it with (ISL) 2013-05, which continues the direction that cleared contractors must report to DSS all breaches of unclassified networks (when related to a classified program), even though "the NISPOM does not cover the protection of unclassified information or information systems." The letter states that "a cyber-intrusion may fall under the reporting requirements of NISPOM … regardless of the classification level of information or information system involved in the intrusion, provided that…(ii) these activities constitute a threat to the protection of classified information, information systems, or programs that are otherwise covered by the NISPOM." The language at section (ii) asserts DSS as the recipient agent for the reporting of cyber intrusions anytime a system containing unclassified information related to a classified program is compromised. The letter concludes with an offer of additional guidance on the NDAA 2013 requirements to "clarify reporting of cyber incidents on contractor information systems" which should "help resolve any confusion or potential overlap of activities under the [Defense Industrial Base Cyber Security and Information Assurance] program, the proposed DFARS revisions, and the NISPOM."

DOD Unclassified Controlled Technical Information

On October 10, 2013, the Secretary of Defense, Chuck Hagel, issued a Memorandum on Safeguarding Unclassified Controlled Technical Information.[24] In this two page document, the Secretary directs the Under Secretary for AT&L to propose an amendment to the Defense Federal Acquisition Regulations Supplement for defense contractors to safeguard unclassified controlled technical information. The Memorandum also tasks the Military Departments to identify critical acquisition and technology programs requiring higher levels of protection.

FAR/DFAR Controls on Contractor Information Systems

On November 18, 2013, the DOD issued a final rule amending the Defense Federal Acquisition Regulation Supplement (DFARS) to add a subpart and associated contract clause to address requirements for safeguarding "unclassified controlled technical information." [25] The final rule requires government contractors to "provide adequate security" for their information systems that contain "controlled technical information," notify the DOD of any "cyber incidents" to such information systems, and flow down these requirements to the contractor's subcontractors and vendors.

The DoD, GSA, and NASA issued a proposed rule to amend the Federal Acquisition Regulation (FAR)[26] to add a new subpart and contract clause for the basic safeguarding of contractor information systems that contain information where non-public USG information will be resident or transit the contractor information systems, applicable to any contract meeting the simplified acquisition thresholds, not the sensitivity of the information. The information system-centric basic protection measures are first-level information technology security measures used to deter

---

[23] National Defense Authorization Act for Fiscal Year 2013, January 3, 2012, available at: http://www.gpo.gov/fdsys/pkg/BILLS-112hr4310enr/pdf/BILLS-112hr4310enr.pdf

[24] Available at: http://www.defense.gov/documents/Signed_DVTT_Memo_101013.pdf.

[25] 78 FR 69273-282 (November 18, 2013). See e.g., Comments 1 and 23 regarding concerns regarding alignment with USG federal-wide CUI policy and conflicts with controls imposed on information controlled by the ITAR and EAR.

[26] 77 FR 51499 (August 24, 2012) https://www.federalregister.gov/articles/2012/08/24/2012-20881/federal-acquisition-regulation-basic-safeguarding-of-contractor-information-systems

unauthorized information compromise, and include things like maintaining malware, using security patches when issued, and avoiding using unsecured computers to access USG information, among others. These basic safeguards for the most part reflect typical business standards for access to information systems, but the safeguarding requirements at 52.204-XX(b)(4) may represent a challenge for companies both large and small, as it additionally requires that contractors "Protect information provided by or generated for the Government … by at least one physical … barrier (e.g., locked container or room, login and password) when not under direct individual control." These physical barrier controls are similar to those required for classified information, and may be difficult to implement. It is noted that the rule "may be altered as necessary to align with any future direction given in response to ongoing efforts led by the National Archives and Records Administration in the implementation of Executive Order 13556…".

Background and History of CPI

Unlike CUI, about which information is readily available in the public domain, very little unclassified or public domain information is available regarding CPI. The DTAG found it difficult to research and understand the CPI process.

CPI Overview

Critical Program Information (CPI) is a unique subset of CUI that has been established over several decades and is best described by Department of Defense (DoD) INSTRUCTION 5200.39 in 2008.[27] Herein, CPI is defined as:

> Elements or components of an RDA program that, if compromised, could cause significant degradation in mission effectiveness; shorten the expected combat-effective life of the system; reduce technological advantage; significantly alter program direction; or enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability.
>
> Includes information about applications, capabilities, processes, and end-items.
> Includes elements or components critical to a military system or network mission effectiveness.
> Includes technology that would reduce the US technological advantage if it came under foreign control.
>
> CPI information shall be identified early in the research, technology development and acquisition processes, but no later than when a DoD Agency or military component demonstrates an application for the technology in an operational setting, in support of a transition agreement with a pre-systems acquisition or acquisition program, or in exceptional cases, at the discretion of the laboratory/technical director.
>
> Pre-systems acquisition and acquisition programs shall review their programs for CPI when technologies are transitioned from research and development or inherited from another program, during the technology development phase, throughout program progression, and as directed by the MDA.

This definition provides a broad definition of "what" is controlled and directs DoD agencies "when" to identify CPI within the acquisition process. It is to be limited to DoD research, development, and acquisition (RDA) programs

[27] Available at: http://www.dtic.mil/whs/directives/corres/pdf/520039p.pdf.

only, and has no bearing on technologies or products not developed with DoD funding, or developed for foreign customers (except when these would "reduce US technological advantage").

In its Defense Acquisition Guidebook,[28] the DoD states, that "[s]implistically…CPI… should be thought of as the technological "crown jewels" of the program. The United States gains military advantages from maintaining technology leads in key areas, so we must protect them from compromise in the development environment and on fielded systems… It may also include Controlled Unclassified Information (CUI), which is official unclassified information that has been determined by designated officials to be exempt from public disclosure, and to which access or distribution limitations have been applied in accordance with national laws and regulations such as the International Traffic in Arms Regulations for U.S. Munitions List items and the Export Administration Regulations for commerce controlled dual-use items."

In practice, the DoD directive is executed by an internal process involving 13 DoD agencies or offices representing various Armed Services / Military Departments and other DoD divisions. These are the:

1. National Disclosure Policy (NDP) - (interagency process)
2. Low Observable/Counter Low Observable (LO/CLO)
3. Anti-Tamper (AT)
4. Committee for Systems National Security (COMSEC) - (interagency process)
5. Special Access Program (SAP)
6. Defensive Systems Committee (DSC)
7. Missile Technology Control Regime (MTCCR) – (interagency process)
8. Night Vision Device / Inertial Navigation Systems (NVD/INS)
9. Intelligence (INTEL) - (interagency process)
10. Data Links/Waveform
11. Positioning, Navigation & Timing, Global Positioning System (PNT/GPS)
12. Geospatial Intelligence (GEOINT) - (interagency process)
13. Electronic Warfare (EW) - (interagency process)

Of these internal processes (sometimes referred to as the "pipes" or "stovepipes"), six are interagency processes, requiring additional coordination, and some have multiple layers of internal review. For example, to adjudicate a LO/CLO technology, [29] up to three levels of review may be involved: (1) an initial review, (2) a Tri-Service Committee Review, and (3) an Executive Committee review by high-ranking commanders.[30]

DoD Internal Review Process for Release/Export of CPI

Over the past 50 years, the DoD established the 13 subgroups identified above to protect CPI and determine releasability for specific types of technologies that are acquired by the USG. These groups are coordinated by the Defense Technology Security Administration (DTSA), through one of its seven directorates, the Technology Security and Foreign Disclosure Office ("TSFDO"), an organization added within the past four years. To aid in the management of its CPI review obligations, the TSFDO created an oversight committee, the Arms Transfer and Technology release Senior Steering Group (ATTR SSG), charged to lead the coordination of positions from these 13 DoD subgroups. The ATTR SSG was established by the Deputy Secretary of Defense in 2008, and includes members from the Military Department, Joint Staff, Office of the Under Secretary of Defense for Intelligence (OUSD(I)),

---

[28] Available at: https://acc.dau.mil/CommunityBrowser.aspx?id=492076.

[29] Governed by DoD Instruction S-5230.28, *Low Observable (LO) and Counter Low Observable (CLO) Programs (U)*, May 26, 2005.

[30] Source: *Technology Security Ruminations*, Maj. Gen. Thomas Masiello, on the web at: http://www.ndiagulfcoast.com/events/archive/38th_symposium/MasielloSymp12.pdf.

National Security Agency (NSA), National Geospatial-Intelligence Agency (NGA), the DoD Chief Information Officer, and is co-chaired by representatives of DoD Policy and DoD Acquisition, Technology, and Logistics (AT&L). In its role, the ATTR SSG provides functional oversight of the 13 DoD subgroups in developing export policy for U.S. technologies, as well as serving as an escalation point if other DoD stakeholders are unable to agree on a policy. Additionally, TSFDO leads the development of ATTR SSG anticipatory policies and releases in principle (RIP), which reflect, inform, or represent high-level decisions regarding technology release and foreign disclosure in anticipation of formal requests for the transfer or release of critical DoD technologies.[31]

The TSFDO offices employs a staff of 9 tasked with supporting the 100-200 priority requests annually that come out of the ~85,000 requests that are routinely administered outside the TSFDO process. These are predominantly comprised of direct commercial sale (DCS) export requests from industry for sales outside of the U.S. foreign military sale (FMS) process.

Additionally, the 13 subgroups providing CPI reviews, and the ATTR SSG coordinating these reviews, do not work directly with the USG agencies tasked with export control and licensing, specifically the Directorate of Defense Trade Controls within the Department of State (DDTC), and Bureau of Industry and Security within the Department of Commerce (BIS). There is no direct connection between the USG export control and licensing agencies accountable for delivering USG policy to industry[32] and the policy team playing a critical role making these determinations.

Within each of the Military Departments / Armed Forces, the subordinate agency responsible for CPI review varies. The Army interface is a subset of AT&L, within the Navy, it is the Navy International Programs Office (NIPO), and for the Air Force, the agency is the Secretary of the Air Force, Office International Affairs (SAF/IA). These three agencies do not employ a standard approach to determining what CPI is and how it should be protected. There are no common criteria for evaluation or procedures followed between the various offices with respect to the CPI technical review. Two processes typically take longer than others, the (1) AT and (2) Electronic Warfare data protection reviews. The DoD has been aware of inefficiencies in its CPI processes and has taken steps to resolve these.

Beginning with Deputy Secretary of Defense William J. Lynn, III (1997-2001) and later Ashton B. Carter (2009-2011), the Office of the Secretary of Defense (OSD) requested reviews of CPI processes. The creation of the TSFDO was one outcome intended to consolidate the processes. Additionally, the Army AT&L office is working on a singular, specific definition of CPI and standardized process to the CPI review in the acquisition process, so that anticipatory policy and release processes are consistent with the ultimate exportability of a technology.

Another DoD goal is to incentivize their program personnel to conduct timely, accurate CPI reviews by linking performance incentives and metrics to high-quality CPI reviews, just as is currently done for personnel who meet or exceed cost and schedule targets.

The most promising reforms are found in the DTSA Strategic Plan 2013. In it, the TSFDO stated its intent to:

- continue the institutionalization of TSFD reforms and processes by codifying the reformed high-level decision (HLD) process in a new DoDD no later than December 15, 2013,
- complete and implement a new ATTR SSG charter that refines TSFD processes and procedures, and
- publish not less than two anticipatory policies per year in accordance with DepSecDef guidance

---

[31] Portions from the DTSA Strategic Plan 2013, on the web at http://www.dtsa.mil/Documents/DTSA_Strat_Plan.pdf.

[32] The policy is typically delivered by the DDTC or the BIS in the form of export licenses and any limitations (provisos or riders and conditions).

among its other objectives. It is also currently tasked with streamlining foreign release process to help industry get through the 13 different CPI stakeholders' review. However, interagency agreement on a singular method has not yet been achieved.

Examples and Challenges of Competing Requirements – CUI and CPI

In keeping with its task, the DTAG working group reached out to colleagues and collected several examples of overreach, confusion, duplicative, and competing requirements involving CUI or CPI. The group was advised of several situations where different agencies imposed different or duplicative requirements (e.g., audit oversight, reporting, and other control measures). In addition, the group learned about confusion existing within industry regarding the CUI and CPI definitions, related policies and processes. Several of the examples obtained through its research are contained in the DTAG Working Group's PowerPoint presentation.

Three common themes arose from multiple industry contacts polled:

1. The multiple variants of CUI, as well as the multiple variants for controlling CUI, create confusion and impose costs on industry. In addition, such factors may give industry pause before accepting USG contracts, especially when special safeguarding requirements mean significant additional costs to recreate segregated data storage and application access tools.
2. Programs subject to CPI review are especially complicated and require specialized personnel to "walk" through the system, and companies without such expertise have difficulty entering the international defense marketplace, even when offering products with broad foreign availability or that are technologically insignificant.
3. When interacting with cleared contractors (e.g., audits), DSS personnel may require information about export licenses, controls for exports, compliance procedures, and other unclassified information related to the ITAR and export-controlled information maintained by the contractor. In certain instances, companies have perceived and/or questioned DSS's role as having oversight of unclassified export controlled information or serving as a monitoring/enforcement arm of the DDTC.

Observations

The DTAG reviewed CUI and CPI in the context of the history, evolution, and current context for these terms and what they mean within the USG, and documented observations unique to its industry perspective.

- Generally, export controlled information, whether controlled under the ITAR or the EAR, is already subject to the access and dissemination controls established by these regulations. Additional marking, safeguarding, licensing and reporting requirements imposed on Technical Data (ITAR) or Technology (EAR) when it is also CUI (and as proposed by the Task Force Report definition of CUI, it is)[33] adds burden, expense, and often confusion to industry members.

- In response to the 2013 NDAA, proposed changes to the NISPOM were made to add the Section 941 language on reporting requirements. These reporting requirements imposed upon cleared defense contractors only a requirement to report to DoD penetrations of certain unclassified networks and information systems, where previously only classified breaches needed to be reported. Industry urged the removal of such language since the NISPOM establishes the rules for handling classified information

[33] Recall that the singular proposed definition is " All unclassified information for which, pursuant to statute, regulation, or departmental or agency policy, there is a compelling requirement for safeguarding and/or dissemination controls." rather that the legacy definition of FOUO which was only concerned with "unclassified information of a sensitive nature, not otherwise categorized by statute or regulation."

and the NDAA language relates to unclassified information. Further, such a change would foster an uneven playing field between companies with and without classified information. NISPOM conforming changes are being considered; there is still industry concern that DSS seeks to fulfill the role established by section 941 of the NDAA 2013.

- The DoD definition of CPI is limited to, "the research, technology development and acquisition processes," "when a DoD Agency or military component demonstrates an application for the technology in an operational setting," or "technology that would reduce the US technological advantage if it came under foreign control." Stated more succinctly, the CPI process, as defined, appears to be limited predominantly to technologies belonging to the DoD. However, in practice, industry finds that the TSFDO primarily conducts CPI reviews for technologies developed by companies, without USG ownership, and to be exported by direct commercial sale (DCS).

- Companies may be reluctant to spend the money to develop USML technologies for the DCS market since the CPI review processes may ultimately result in prohibiting these items' export, possibly even after CPI requirements are met.

- It is not uncommon for the CPI review process to take several months to return a determination regarding the ability to release or export CPI. In addition, the various DoD offices involved in the CPI review process often do not coordinate effectively. For industry awaiting a policy decision in order to take action, such as respond to a foreign bid opportunity, a great deal of risk goes into any decision to invest the time and resources to begin preparing a response. If the company avoids the risk of rejection by delaying efforts until the export is approved, it may not have enough time to prepare an adequate response. Anytime the export license is not authorized (or is approved, but the approval is so limited it is essentially a denial) all the investment of time, work, and resources allocated to preparing for the potential sale (marketing, engineering, proposal preparation, etc.) is lost.

- The ATTR SSG is charged to come up with "high level decisions." These include anticipatory policy and a consolidated release processes to harmonize the 13 subgroups' inputs so that industry could receive timely anticipatory guidance and make a determination of the risk in pursuing an international opportunity.

- Industry does not have insight as to the DoD offices or departments that control technical release policies and determinations. Only by direct meetings can the (current) "policy" be determined. Changes to the CPI/technical release policy or licensing policy are not collectively communicated or available to industry. This process is very discouraging; especially for small-to-medium sized companies who may want to compete with their defense products but don't have the resources to assign personnel to develop relationships and pre-coordinate positions with all the various DoD stakeholders.

- Changes to the acquisition process, such as those made by the DoD, GSA, and NASA to the FAR via 77 FR 51499, and the creation of new categories of sensitive information with unique control requirements, such as the safeguarding requirements for "unclassified controlled technical information" recently requested by the Secretary of Defense, only serve to confuse the already overwhelmed private sector attempting to make sense of all its obligations with respect to USG information. With over 117 terms already in play, keeping track of all the competing requirements creates an opportunity for industry error in either misidentify or incorrectly controlling certain information. A move toward consistency and standardize is much needed.

Recommendations

The DTAG recognizes the considerable undertaking by the USG to consolidate CUI under the Executive Agent and as recommended by the CUI Task Force, and acknowledges that significant progress has been made to date. The DTAG encourages the continued work of USG to improve the standardization and controls associated with CUI, and welcomes any opportunity to support or assist in these improvements.

It is the DTAG recommendation that export-controlled Technical Data and Technology not be subject to duplicative CUI requirements (e.g., whether they relate to licensing, marking, auditing, reporting), as these may have costly implications for industry and also will likely have the unintended consequence of creating multiple overlapping and potentially competing or conflicting safeguarding requirements. The DTAG recommends that DDTC coordinate with other agencies with potentially overlapping definitions and controls (e.g., DSS, NSA) to coordinate their objectives and requirements on industry to prevent or minimize duplicative and conflicting CUI requirements.

The DTAG believes that many of the efforts relating to the CUI consolidation process may also be useful in addressing the CPI definitional and process issues, and that DDTC should support the DTAG/ATTR SSG in its efforts to provide timely, regular anticipatory policy to industry.

With respect to DoD's protection of CPI and the operations of the TDSFO and ATTR STTG, the DTAG believes that it would benefit many exporters if DDTC and DTSA make available a basic overview of these committees, their areas of jurisdiction, the types of applications that are of concern to them, and – if possible – a contact person. Much of the substantive work of these committees is classified, but there should be some general information that could be disseminated to provide general notice and a description of the process to exporters involved in technologies that might be subject to these review processes. One option would be to include an overview of the committee and the process on the DDTC website or in DDTC licensing guidance.

DOC/BIS (Department of Commerce/Bureau of Industry & Security)			
Definitions and Examples of CUI	**Definition of CPI**	**Statutory/Regulatory Authority**	**Agency Policy/Directive**
"Technology": "the information and know-how (whether in tangible form, such as models, prototypes, drawings, sketches, diagrams, blueprints, or manuals, or in intangible form, such as training or technical services) that can be used to design, produce, manufacture, utilize, or reconstruct goods, including computer software and technical data, but not the goods themselves." 50 U.S.C. App. § 2415(4) *See also* 15 C.F.R. § 772.1, defining "Technology" (General Technology Note) as: "Specific information necessary for the 'development', 'production', or 'use' of a product. The information may take the form of 'technical data' or 'technical assistance.'" "Technical data": "May take forms such as blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and instructions written or recorded on other media or devices such as disk, tape, read-only memories." 15 C.F.R. § 772.1 "Technical assistance": "May take forms such as instruction, skills training, working knowledge, consulting services." 15 C.F.R. § 772.1 "Controlled Technology," General Technology Note (Supp. No. 2 to Part 774) and the Commerce Control List (Supp. No. 1 to Part 774) "Section 12(c) Information," Supp. No. 2 to Part 736—Administrative Orders	None	Export Administration Act ("EAA") of 1979, as amended (50 U.S.C. App. § 2401 et seq.), extended under the authority of the International Emergency Economic Powers Act (50 U.S.C. § 1701 et seq.) Export Administration Regulations ("EAR"), 15 C.F.R. §§ 730-774 Section 12(c) of the EAA (50 U.S.C. App. § 2411(c)) Exec. Order No. 11,958 §§ 1(*l*)(3), 2(a) (Jan. 18, 1977) (revoked by Exec. Order No. 13,637 (Mar. 8, 2013), "except that, to the extent consistent with this order, all determinations, authorizations, regulations, rulings, certificates, orders, directives, contracts, agreements, and other actions made, issued, taken, or entered into under the provisions of Executive Order 11958, as amended, and not revoked, superseded, or otherwise made inapplicable, shall continue in full force and effect until amended, modified, or terminated by appropriate authority.") 22 C.F.R. § 120.4 (Commerce participation with State/DDTC in commodity jurisdiction requests)	Administrative Order One: Disclosure of License Issuance and Other Information (Supplement No. 2 to 15 C.F.R. § 736)"[I]nformation obtained by the U.S. Department of Commerce for the purpose of consideration of or concerning license applications"

DHS (Department of Homeland Security)			
Definitions and Examples of CUI	**Definition of CPI**	**Statutory/Regulatory Authority**	**Agency Policy/Directive**
"CUI": "Information that is not deemed to be Classified Information in the United States, but to which access or distribution limitations have been applied in accordance with national laws, regulations, policies, or directives of either Party." See e.g., "Agreement Between the Government of the United States of America and the Government of New Zealand on Science and Technology Cooperation Contributing to Domestic and External Security Capabilities" (Jan. 8, 2010). CUI includes: • "Sensitive Homeland Security Information" (*see* 6 U.S.C. § 482(f)(1) (defining "Homeland Security Information")) • "Sensitive Security Information" (*see* 49 C.F.R. § 1520.5) • "For Official Use Only" (FOUO) • "Law Enforcement Sensitive Information" • "Protected Critical Infrastructure Information" (*see below*) • "Restricted" • "Trusted Information Sharing Network for Critical Infrastructure Protection (TISN) In Confidence" • "In Confidence" • "Sensitive" "Protected Critical Infrastructure Information" (PCII): "all critical infrastructure information, including categorical inclusion PCII, that has undergone the validation process and that the PCII Program Office has determined qualifies for protection under the CII Act." DHS, Protected Critical Infrastructure Information Program Procedures Manual (Apr. 2009) "Chemical-terrorism vulnerability information" (CVI), 6 C.F.R. § 27.400 "Critical Infrastructure Information" (CII), Critical Infrastructure Act of 2002 § 212(3), *see also* 6 C.F.R. § 29.2 "Personally Identifiable Information" (PII) and "Sensitive Personally Identifiable Information," DHS, "Handbook for Safeguarding Sensitive Personally Identifiable Information" (Mar. 2012)	N/A	Executive Order No. 13,286 § 54 (Feb. 28, 2003) (as amended), amending Executive Order No. 12,002 (July 7, 1977) § 3 (adding the Secretary of Homeland Security to the Export Administration Review Board) National Security Presidential Directive – 56, "Defense Trade Reform" (Jan. 22, 2008) (providing for DHS participation in commodity jurisdiction determinations: "The Secretary of Homeland Security (or the Secretary's designee) shall participate whenever compliance, enforcement, and specific commodity jurisdiction issues relating to technologies of homeland security concerns, as well as other issues as determined by the Secretary of State, are addressed," *cited in* Committee on Homeland Security and Export Controls; Development, Security, and Cooperation; Policy and Global Affairs; National Research Council, "Export Control Challenges Associated with Securing the Homeland," at 39 (2012)) Exec. Order No. 13,558 (Nov. 9, 2010) (directing the Secretary of Homeland Security to establish "an interagency Federal Export Enforcement Coordination Center" which, among other duties, will "serve as a primary point of contact between enforcement authorities and agencies engaged in export licensing") 22 C.F.R. § 127.4 (Immigration & Customs Enforcement and Customs & Border Protection "may take appropriate action to ensure observance of this subchapter as to the export or the attempted export or the temporary import of any defense article or technical data . . .")	DHS Management Directive 11042.1, "Safeguarding Sensitive but Unclassified Information" (Jan. 6, 2005) DHS, "Protected Critical Infrastructure Information Program Procedures Manual" (Apr. 2009) DHS, "Handbook for Safeguarding Sensitive Personally Identifiable Information" (Mar. 2012)

DOD (Department of Defense)			
Definitions and Examples of CUI	**Definition of CPI**	**Statutory/Regulatory Authority**	**Agency Policy/Directive**
"CUI": "Information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, excluding information that is classified under E.O. 13526 of December 29, 2009, or the Atomic Energy Act of 1954, as amended. (P.L. 83-703)." DSCA Manual 5105.38-M (SAMM), Chapter 3, Table C3.T1 (2013) "Controlled technical information," 48 C.F.R. § 204.7301, Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified Controlled Technical Information (DFARS Case 2011-D039), Final Rule (78 Fed. Reg. 69273, 69279; Nov. 18, 2013) "Technical information," 48 C.F.R. § 204.7301, 78 Fed. Reg. 69279-80 "Technical data," 48 C.F.R. § 252.227-7013(15) "Technical data with military or space application," 10 U.S.C. § 130(c) "DOD Unclassified Controlled Nuclear Information," 32 C.F.R. § 223.3(c) "Unclassified information pertaining to security measures, including security plans, procedures, and equipment for the physical protection of special nuclear material," 10 U.S.C. § 128(a)(1)	"CPI": "Elements or components of a Research Development, and Acquisition program that, if compromised, could cause significant degradation in mission effectiveness; shorten the expected combat-effective life of the system; reduce technological advantage; significantly alter program direction; or enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability. Includes information about applications, capabilities, processes, and end-items. Includes elements or components critical to a military system or network mission effectiveness. Includes technology that would reduce the US technological advantage if it came under foreign control." DoDI 5200.36 "Critical Program Information (CPI) Protection within the Department of Defense" (Jul. 16, 2008, modified Dec. 28, 2010; SAMM, Chapter 3, Table C3.T1	Exec. Order No. 11,958 §§ 1(*l*), 2(a) (Jan. 18, 1977) (revoked by Exec. Order No. 13,637 (Mar. 8, 2013), "except that, to the extent consistent with this order, all determinations, authorizations, regulations, rulings, certificates, orders, directives, contracts, agreements, and other actions made, issued, taken, or entered into under the provisions of Executive Order 11958, as amended, and not revoked, superseded, or otherwise made inapplicable, shall continue in full force and effect until amended, modified, or terminated by appropriate authority.") **License Application Review** • 22 U.S.C. §§ 2797(a)–(b); 2778(g)(8); 2778 note ("Effective Regulation of Satellite Export Activities") • 50 U.S.C. app. §§ 2404(a)(1), 2405(a)(1) • 15 C.F.R. § 750.3(b) • 22 C.F.R. § 124.15(a)(1) **License Exceptions** • 22 C.F.R. §§ 125.4(b)(1), (b)(3); 125.4(c); 125.5(a); 126.4(a), (c); 126.6(a), (c) **Authority to Withhold/Prevent** • 10 U.S.C. §§ 128(a), 130(a) **Commodity Jurisdiction** • 22 C.F.R. §§ 120.4 Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified Controlled Technical Information (DFARS Case 2011-D039), Final Rule (78 Fed. Reg. 69273; Nov. 18, 2013).	DoDI 5230.24, "Distribution Statements on Technical Documents" (Aug. 23, 2012) DoDD 5230.25, "Withholding of Unclassified Technical Data from Public Disclosure" (Nov. 6, 1984, modified Aug. 18, 1995) DoDM 5200.01, Vol. 4, DoD Information Security Program: Controlled Unclassified Information (Feb. 24, 2012) DoDI 8582.01, "Security of Unclassified DoD Information on Non-DoD Information System" (Jun. 6, 2012)

DOD/DSS (Defense Security Service)			
Definitions and Examples of CUI	**Definition of CPI**	**Statutory/Regulatory Authority**	**Agency Policy/Directive**
The definition of CUI presumably is the same as for DOD: SAMM "provides DoD-wide guidance" and "is mandatory for use by all DoD Components." Examples from NISPOM: • "Critical Technology," § 2-300 • "Export-controlled information," § 5-508 • "Unclassified information," §§ 5-511, 7-101, 10-303 • "Information Controlled by Originator" (ORCON), § 9-303(a) • "For Official Use Only" (FOUO), § 9-303(b) • "Proprietary Information Involved" (PROPIN), § 9-303(c) • "Technical data," § 10-101, Appendix C • "In Confidence Information" (from foreign governments), § 10-303 • "Restricted" (unless bilateral security agreement requires classified protection), § 10-303 • "Militarily Critical Technical Data," § 11-202(b) "Sensitive Technology" and "Sensitive Information," *Targeting Technologies: A Trend Analysis of Reporting from Defense Industry*, at 9 (2012)	The definition of CPI presumably is the same as for DOD: SAMM "provides DoD-wide guidance" and "is mandatory for use by all DoD Components."	Exec. Order No. 12,829 (Jan. 6, 1993) (as amended) (establishes a National Industrial Security Program to safeguard Federal Government classified information that is released to contractors, licensees, and grantees of the United States Government). 22 C.F.R. §§ 125.3(a), 125.9, 127.5 (authority to authorize the export of *classified* technical data and *classified* defense articles) DSS is a member of the Export Enforcement Coordination Center, which is supposed to "serve as a primary point of contact between enforcement authorities and agencies engaged in export licensing." Exec. Order No. 13,558 (Nov. 9, 2010)	DoDM 5220.22-M, "National Industrial Security Program Operating Manual" (NISPOM) § 10-408(b) (Feb. 28, 2006, modified Mar. 28, 2013) (*see, e.g.*, §§ 2-300, 5-508, 5-511, 7-101, 9-303, 10-101, 10-303, 10-509, and 11-202) DoDD 5105.42, § 5(a)(4) "Defense Security Services" (Aug. 3, 2010; modified Mar. 31, 2011) ("Administer *classified* export authorizations related to direct commercial sales and foreign military sales, as required by . . ." ITAR) (emphasis added) Industrial Security Letters (*See* 96L-1, 2006-02, 2013-03) [Note: DSS has stated: "Certain basic principles of international security apply to both classified and unclassified information. These principles are included in Chapter Ten for information only and are not intended to apply security countermeasures to unclassified information except as otherwise required pursuant to the ITAR, contracts, or international agreements. For example: . . . unclassified export controlled information may be included in a Technology Control Plan if required by a State Department export authorization or by contract." ISL 96L-1. While almost decades old, this ISL was issued before the most recent NISPOM was released, but suggests that DSS may derive some authority over unclassified information from its NISPOM responsibilities regarding Technology Control Plans.]

DOD/DTSA (Defense Technology Security Administration)			
Definitions and Examples of CUI	**Definition of CPI**	**Statutory/Regulatory Authority**	**Agency Policy/Directive**
The definition of CUI presumably is the same as for DOD.	The definition of CPI presumably is the same as for DOD.	10 U.S.C. §§ 113(d), 134(b)(3)	DoDD 5105.72, "Defense Technical Information Center," § 5.1.3.1 (July 28, 2005)

DOD/NGA (National Geospatial-Intelligence Agency)			
Definitions and Examples of CUI	**Definition of CPI**	**Statutory/Regulatory Authority**	**Agency Policy/Directive**
The definition of CUI presumably is the same as for DOD.	The definition of CPI presumably is the same as for DOD.	**License Application Review** 22 U.S.C. § 2778 note ("Effective Regulation of Satellite Export Activities") **License Exceptions** Presumably the same as for DoD, subject to NISPOM	**General Authority** DoDD 5105.60, "National Geospatial-Intelligence Agency (NGA)," Enclosure 2, § (e)(14) (July 29, 2009) **License Exceptions** NISPOM, § 10-408(b)

DOD/NSA			
Definitions and Examples of CUI	**Definition of CPI**	**Statutory/Regulatory Authority**	**Agency Policy/Directive**
The definition of CUI presumably is the same as for DOD.	The definition of CPI presumably is the same as for DOD.	**License Application Review** 22 U.S.C. § 2778 note ("Effective Regulation of Satellite Export Activities"); note ("Satellite Export Controls," at "Sec. 1514. National Security Controls on Satellite Export Licensing"); note ("Proliferation and Export Controls," at "Sec. 1411. Enhanced Intelligence Consultation on Satellite License Applications") 22 C.F.R. § 124.15(a)(1) **License Exceptions** Presumably the same as for DoD, subject to NISPOM	**License Exceptions** NISPOM, § 10-408(b) *See also* NSA/Central Security Service/Office of Export Control Policy (re SIGINT and Information Assurance sensitive technologies) and NSA Technology Transfer Program Office

Department of Energy (DOE)			
Definitions and Examples of CUI	**Definition of CPI**	**Statutory/Regulatory Authority**	**Agency Policy/Directive**
Technology subject to Part 810 Regulations (Source: 10 C.F.R. 810.2) "Sensitive nuclear technology" (Source: 10 C.F.R. 810.3) "Unclassified controlled nuclear information": "certain unclassified Government information concerning nuclear facilities, materials, weapons, and components whose dissemination is controlled under section 148 of the Atomic Energy Act and this part." 10 C.F.R. § 1017.4 "Sensitive Subjects List" (internal use). (*See* Lawrence Berkeley National Laboratory, U.S. Department of Energy) ; see also, Order Code RL33303, CRS Report for Congress, "Sensitive But Unclassified" Information and Other Controls: Policy and Options for Scientific and Technical Information) "Official Use Only" (OUO)	N/A	Atomic Energy Act of 1954, P.L. 83-73, sec. 57(b), amended by Nuclear Nonproliferation Act of 1978 Assistance to Foreign Atomic Energy Activities (Part 810 Regulations), 10 CFR Part 810. [Note: 10 CFR § 810 is being amended, including sections concerning export license applications and interagency review. *See* 78 Fed. Reg. 46829 (Aug. 2, 2013)] "Dissemination of unclassified information," 42 U.S.C. § 2168(a) "Nuclear related controls," 22 C.F.R. § 123.20 "Identification and Protection of Unclassified Controlled Nuclear Information," 10 C.F.R. § 1017 15 C.F.R. § 750.3(b)-Authority of agencies (including DOE) to review license applications submitted to BIS. Executive Order No. 12,755 § 1 (Mar. 12, 1991), amending § 3 of Executive Order No. 12,002 (July 7, 1977) (adding the Secretary of Energy to the Export Administration Review Board) 15 C.F.R. § 772.1 (*see* "Advisory Committee on Export Policy" and "Operating Committee," listing officials from the Department of Energy on both committees.	DOE O 471.1B, "Identification and Protection of Unclassified Controlled Nuclear Information" (Mar. 1, 2010); (https://www.directives.doe.gov/directives/0471.1-BOrder-b/at_download/file) *DOE Sensitive Subjects List* http://www.lbl.gov/ehs/ops/ufva/doc/SensitiveSubjectsList_Sept01.pdf

DOJ/DEA (Department of Justice/Drug Enforcement Administration)			
Definitions and Examples of CUI	**Definition of CPI**	**Statutory/Regulatory Authority**	**Agency Policy/Directive**
From U.S. Department of Justice, Office of the Inspector General, Evaluation and Inspections Division, "Review of the Department of Justice's Reporting Procedures for Loss of Sensitive Electronic Information," Appendix IV (June 2007): • "DEA Sensitive" • "Sensitive But Unclassified" (SBU) • "Law Enforcement Sensitive" (LES) • "For Official Use Only" (FOUO) • "Personally Identifiable Information" (PII)	N/A	15 C.F.R. Supplement No. 3 to Part 730 (stating that DEA has export control responsibilities over chemicals and controlled substances)	*OMB Memorandum M-06-19*, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments" (July 12, 2006), adopted by DEA's CIO and DEA's Chief Inspector (Oct. 12, 2006 email) "DEA National Security Information Classification Guide" (See U.S. Department of Justice "Fundamental Classification Guidance Review, July 2012 (pg. 2)) U.S. Department of Justice, Office of the Inspector General, Evaluation and Inspections Division, "Review of the Department of Justice's Reporting Procedures for Loss of Sensitive Electronic Information," Appendix IV (June 2007)

DOJ/FBI (Department of Justice, Federal Bureau of Investigation)			
Definitions and Examples of CUI	**Definition of CPI**	**Statutory/Regulatory Authority**	**Agency Policy/Directive**
From the FBI's CJIS Security Policy (Department of Justice, Federal Bureau of Investigations, "Criminal Justice Information Services (CJIS) Security Policy," Version 5.2 (Aug. 9, 2013), CJISD-ITS-DOC-08140-5.2, Prepared by: CJIS Information Security Officer, Approved by: CJIS Advisory): • "Criminal Justice Information" (CJI), § 4.1 • "Criminal History Record Information" (CHRI) § 4.1.1 (*see* 28 C.F.R. § 20.3(d)) • "Personally Identifiable Information" (PII), § 4.3 • "Sensitive But Unclassified" (SBU), Appendix A. SBU includes many designations, such as: o "For Official Use Only" (FOUO) o "Law Enforcement Sensitive" (LES) o "Sensitive Homeland Security Information" (SHSI) o "Security Sensitive Information" (SSI) o "Critical Infrastructure Information" (CII)	None	15 C.F.R. § 772.1 ("Advisory Committee on Export Policy" and "Operating Committee," listing DOJ as a member of both committees for "encryption exports;" the Bureau of Industry & Security (at page 9) says that DOJ/FBI is a member of the Operating Committee for encryption cases) Executive Order No. 13,026 § 1(b)(1) (Nov. 15, 1996), amending Executive Order No. 12,981 (Dec. 5, 1995) (permitting DOJ to review export license applications for encryption products submitted to Commerce; also adding DOJ to the Export Administration Review Board) However, the same Executive Order says: "Because the export of encryption software, like the export of other encryption products described in this section, must be controlled because of such software's functional capacity, rather than because of any possible informational value of such software, such software *shall not be considered or treated* as 'technology,' as that term is defined in section 16 of the EAA (50 U.S.C. App. 2415) and in the EAR (61 Fed. Reg. 12714, March 25, 1996)" (*Id.*, § 1(c)) (emphasis added) Executive Order No. 13,558 (Nov. 9, 2010) (directing the Secretary of Homeland Security to establish "an interagency Federal Export Enforcement Coordination Center" which, among other duties, will "serve as a primary point of contact between enforcement authorities and agencies engaged in export licensing;" the Executive Order requires the DOJ's membership and the Center's web site lists the FBI as a participating agency)	"FBI National Security Information Security Classification Guide" (See U.S. Department of Justice "Fundamental Classification Guidance Review, July 2012 (pg. 2)) Department of Justice, Federal Bureau of Investigations, "Criminal Justice Information Services (CJIS) Security Policy," Version 5.2 (Aug. 9, 2013), CJISD-ITS-DOC-08140-5.2, Prepared by: CJIS Information Security Officer, Approved by: CJIS Advisory) U.S. Department of Justice, Office of the Inspector General, Evaluation and Inspections Division, "Review of the Department of Justice's Reporting Procedures for Loss of Sensitive Electronic Information," Appendix VI (June 2007)

Federal Energy Regulatory Commission (FERC)			
Definitions and Examples of CUI	**Definition of CPI**	**Statutory/Regulatory Authority**	**Agency Policy/Directive**
"Critical Energy Infrastructure Information" (CEII) (Source: Order Code RL33303, CRS Report for Congress, "Sensitive But Unclassified" Information and Other Controls: Policy and Options for Scientific and Technical Information)	N/A	Federal Power Act, 15 USC. 717 *et. seq.* Natural Gas Act, 16 USC 791a, *et. seq.* FERC Information and Requests Regulations, 18 USC 388.113	*FERC Order No. 683, CEEI Final Rule* http://www.ferc.gov/whats-new/comm-meet/092106/M-2.pdf *FERC Order No. 630 – CEEI Final Rule* http://elibrary.ferc.gov/idmws/common/opennat.asp?fileID=9639612 *FERC Order No. 630-A – CEEI Final Rule* http://elibrary.ferc.gov/idmws/common/opennat.asp?fileID=9745149 *FERC Docket No. PL01-2-000, Statement of Policy on Treatment of Previously Public Documents* http://www.ferc.gov/legal/maj-ord-reg/land-docs/97ferc61030.pdf

Nuclear Regulatory Commission (NRC)			
Definitions and Examples of CUI	**Definition of CPI**	**Statutory/Regulatory Authority**	**Agency Policy/Directive**
"Safeguards Information" (SGI): Information concerning the physical protection of operating power reactors, spent fuel shipments, strategic special nuclear material, or other radioactive material, the unauthorized disclosure or which could reasonably be expected to have a significant adverse effect on the health and safety of the public by increasing the likelihood of sabotage or theft of special nuclear material • "Sensitive unclassified non-safeguards information" (SUNSI): Information that is generally not publicly available and encompasses seven categories: 1. Allegation Information 2. Investigation Information 3. Proprietary Information 4. Privacy Act Information 5. Security-Related Information (e.g., information about a licensee's or applicant's physical protection or material control and accounting program for special nuclear material not otherwise designated as SGI or Classified) 6. Sensitive Internal Information 7. Federal-, State-, Foreign Government-and International Agency Controlled Information	N/A	SGI: Section 147 of the Atomic Energy Act of 1954, as amended (added by P.L. 96-295, §207(a)(1) (1980); codified in 42 USC §2167).; 10 CFR 73.21-73.23 SUNSI: 10 CFR §2.390(d)(1) (withholding security-related information from public disclosure) [Note: 10 CFR Part 110 generally controls export and import of equipment and materials, not Technical Data, which is regulated by DOE. See 10 CFR Part 810]	**SGI**: *RIS 2003-08 - Protection of Safeguards Information from Unauthorized Disclosure* http://www.nrc.gov/reading-rm/doc-collections/gen-comm/reg-issues/2003/ri200308.pdf **SUNSI**: *RIS 2005-26-Control of Sensitive Unclassified Non-Safeguards Information Related to Nuclear Power Reactors* http://www.nrc.gov/reading-rm/doc-collections/gen-comm/reg-issues/2005/ri200526.pdf *RIS 2005-31-Control of Security-Related Sensitive Unclassified Non-Safeguards Information Handled by Individuals, Firms, and Entities Subject to NRC Regulation of the Use of Source, Byproduct, and Special Nuclear Material* http://www.nrc.gov/reading-rm/doc-collections/gen-comm/reg-issues/2005/ri200531.pdf

OFAC (Department of Treasury, Office of Foreign Assets Controls)			
Definitions and Examples of CUI	**Definition of CPI**	**Statutory/Regulatory Authority**	**Agency Policy/Directive**
None of the programs that apply to exports/trade transactions defines "technology" or "information" that is subject to controls.	N/A	Congress limited the ability to regulate the export of "informational materials" via the 1998 Berman Amendments to the Trading With the Enemy Act ("TWEA"), 50 U.S.C. App. § 5(b)(4) and the International Emergency Economic Powers Act ("IEEPA") that 50 U.S.C. § 1702(b) and subsequently expanded by the Foreign Relations Authorization Act, Fiscal Years 1994 and 1995, Pub. L. No. 103-236, § 525, 108 Stat. 382, 474 (1994) (amending 50 U.S.C. App. § 5(b) and 50 U.S.C. § 1702(b)) Regulatory definitions of "informational materials" found, for example, in 31 C.F.R. § 560.315(a) (Iran); 31 C.F.R. § 515.332 (Cuba); and 31 C.F.R. § 538.306 (Sudan).	Guidance on Informational Materials (Iran); Internet Access to Informational Materials (Iran); and Substantive Enhancement of Information (Iran) OFAC has limited the exemption by asserting that it does not "exempt from regulation or authorize transactions related to information or informational materials not fully created and in existence at the date of the transactions, or to the substantive or artistic alteration or enhancement of informational materials, or to the provision of marketing and business consulting services." *See, e.g.*, 31 C.F.R. § 560.210(c)(2) (Iran); 31 C.F.R. § 515.206(a)(2) (Cuba); and 31 C.F.R. § 538.212(b)(2). OFAC also notes that the exemption does not authorize the export of any technology subject to the EAR.