PROGRAM MATERIALS
Program #36110
July 20, 2026

Cybersecurity Compliance

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 150, Boca Raton, FL 33487
Phone 561-241-1919

Watson & Associates, LLC
Attorneys | Consultants

Cybersecurity Compliance



July 20, 2026

By Wojciech Z. Kornacki, Esq.

Lecturer

Not Legal Advice / For Educational Purposes Only

Watson & Associates, LLC
Attorneys | Consultants

Agenda

What are my cyber security obligations under the Federal Acquisition Regulation and agency supplements?

What do I do if there was a breach and how much time do I have to report it?

What can I learn from other federal contractors who experienced enforcement actions for cyber security non-compliance?

Watson & Associates, LLC
Attorneys | Consultants

Sources

The Federal Acquisition Regulation

Defense Federal Acquisition Regulation Supplement

NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*

NIST SP 800-172, *Enhanced Security Requirements for Protecting Controlled Unclassified Information*

Executive Order 13556 -- *Controlled Unclassified Information*

https://www.gsa.gov/technology/government-it-initiatives/cybersecurity

https://dibnet.dod.mil

Watson & Associates, LLC
Attorneys | Consultants

Cybersecurity Non-Compliance

Three Russian Nationals and Two Companies Indicted for International Cybercrimes Resulting in More Than $62M in Victim Losses

"From their overseas haven, these defendants ran the criminal infrastructure that powered attacks on critical institutions across our nation," said Assistant Attorney General A. Tysen Duva of the Justice Department's Criminal Division. "Their actions put the American public at risk. We will continue to dismantle these networks and protect our critical infrastructure from cybercriminals at home and abroad."

"The victims in this case are not only in Ohio, but also in 20 other states across the country, touching every aspect of Americans' lives.

Watson & Associates, LLC
Attorneys | Consultants

Cybersecurity Non-Compliance

Contempt Proceedings for Failure to Comply with a Search Warrant Conclude with Vercel Inc., Admitting Wrongdoing and Agreeing to Pay Government's Costs

On Aug. 11, 2025, U.S. Magistrate Judge Ryan Carson issued a search warrant requiring Vercel to disclose the contents of a specified user account in its possession, custody, and control. Three days after Vercel received the search warrant, but prior to Vercel taking any action to execute the warrant, the user deleted the account. Although the deleted information was still located in Vercel's servers in a deletion queue, Vercel did not recover that information and only provided the Government with some records associated with the account. Vercel failed to meet its obligations to produce the entire contents of the account, believing and representing to the court that the records had been deleted.

Watson & Associates, LLC
Attorneys | Consultants

Cybersecurity Non-Compliance

Justice Department Announces Seizure of Stolen-Password Database Used in Bank Account Takeover Fraud

According to the affidavit filed in support of the domain seizure, the criminal group perpetrating the bank account takeover fraud delivered fraudulent advertisements through search engines, including Google and Bing. These fraudulent advertisements imitated the sponsored search engine advertisements used by legitimate banking entities. While the fraudulent advertisements appeared to send users to the websites of legitimate banks, victims were in fact redirected to fake bank websites controlled by the criminals. When victims entered their login credentials to access their bank accounts, the criminals harvested those credentials through a malicious software program embedded in the fake website. The criminals then used those bank credentials on the corresponding legitimate bank websites to access victims' bank accounts and drain their funds.

Watson & Associates, LLC
Attorneys | Consultants

Cybersecurity Non-Compliance

United Kingdom National Charged in Connection with Multiple Cyber Attacks, Including on Critical Infrastructure

According to the complaint, Thalha Jubair, also known as "EarthtoStar," "Brad," "Austin," and "@autistic," 19, of London, England, conspired with others to use social engineering techniques to gain unauthorized access into the computer networks of U.S. companies, steal and encrypt information, and demand ransom payments from victims in exchange for regaining control and preventing the dissemination of the exfiltrated data. Jubair also conspired with others to launder the funds obtained through this scheme. In October 2024 and January 2025, Jubair participated in a scheme to gain unauthorized access to the networks of a U.S.-based critical infrastructure company and the U.S. Courts.

Watson & Associates, LLC
Attorneys | Consultants

Cybersecurity Non-Compliance

Florida Ransomware Negotiator Who Extorted and Attacked Multiple U.S. Victims Sentenced to Prison

“He was hired to help victims in a moment of crisis,” said U.S. Attorney Jason A. Reding Quiñones for the Southern District of Florida. “Instead, Martino betrayed them, fed their confidential negotiating positions to ransomware criminals, and helped squeeze them for more money.

Watson & Associates, LLC
Attorneys | Consultants

Cybersecurity Non-Compliance

Defense contractor LOGZONE Inc. of Huntsville, Alabama has agreed to pay $507,144 to resolve its liability under the False Claims Act for knowingly failing to comply with cybersecurity requirements in contracts with the Department of the Navy.

From May 2021 to March 2025, LOGZONE allegedly failed to implement certain cybersecurity controls in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 that, if not implemented, could lead to significant exploitation of the system or exfiltration of sensitive defense information

Watson & Associates, LLC
Attorneys | Consultants

Cybersecurity Non-Compliance

Georgia Tech Research Corporation Agrees to Pay $875,000 to Resolve Civil Cyber-Fraud Litigation

The settlement resolves a lawsuit against GTRC and Georgia Tech where the United States alleged that until December 2021, those entities failed to install, update or run anti-virus or anti-malware tools on desktops, laptops, servers and networks at Georgia Tech's Astrolavos Lab while the lab conducted sensitive cyber-defense research for DoD. The United States also alleged that until at least February 2020, there was no system security plan in place for the Astrolavos Lab to set out the cybersecurity controls that GTRC's contracts required.

Finally, the United States alleged that in December 2020 GTRC and Georgia Tech submitted a false summary level cybersecurity assessment score to DoD which supposedly applied campus-wide. That summary level score of 98 was allegedly false because (1) there was no campus-wide IT system at Georgia Tech and (2) the score was premised on a "fictitious" or "virtual" environment and did not apply to any actual covered contracting system at Georgia Tech that would process, store or transmit covered defense information.

Watson & Associates, LLC
Attorneys | Consultants

Cybersecurity Non-Compliance

Illumina Inc. has agreed to pay $9.8 million to resolve allegations that it violated the False Claims Act when it sold to federal agencies certain genomic sequencing systems with cybersecurity vulnerabilities.

The settlement resolves allegations that, between February 2016 and September 2023, Illumina sold government agencies genomic sequencing systems with software that had cybersecurity vulnerabilities, without having an adequate security program and sufficient quality systems to identify and address those vulnerabilities. Specifically, the United States contended that Illumina knowingly failed to incorporate product cybersecurity in its software design, development, installation, and on-market monitoring; failed to properly support and resource personnel, systems, and processes tasked with product security; failed to adequately correct design features that introduced cybersecurity vulnerabilities in the genomic sequencing systems; and falsely represented that the software on the genomic sequencing systems adhered to cybersecurity standards, including standards of the International Organization for Standardization and National Institute of Standards and Technology.

Watson & Associates, LLC
Attorneys | Consultants

Cybersecurity Non-Compliance

Defense contractor Aero Turbine Inc., of Stockton, California, and private equity company Gallant Capital Partners LLC, of Los Angeles, have agreed to pay $1.75 million to resolve their liability under the False Claims Act for knowingly failing to comply with cybersecurity requirements in an Aero Turbine contract with the Department of the Air Force.

From June to July 2019, Aero Turbine and Gallant allegedly failed to control the flow of, and limit unauthorized access to, sensitive defense information by providing a software company based in Egypt with files containing such information, even though the software company and its foreign citizen personnel were not authorized to receive sensitive defense information under the Air Force contract.

Watson & Associates, LLC
Attorneys | Consultants

Cybersecurity Non-Compliance

Defense Contractor MORSECORP Inc. Agrees to Pay $4.6 Million to Settle Cybersecurity Fraud Allegations

From January 2018 to September 2022, MORSE used a third-party company to host MORSE's emails without requiring and ensuring that the third party met security requirements equivalent to the Federal Risk and Authorization Management Program Moderate baseline and complied with the Department of Defense's requirements for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis and cyber incident damage assessment;

From January 2018 to January 2021, despite the contracts' system security plan requirement, MORSE did not have a consolidated written plan for each of its covered information systems describing system boundaries, system environments of operation, how security requirements are implemented and the relationships with or connections to other systems;

Watson & Associates, LLC
Attorneys | Consultants

Cybersecurity Non-Compliance

Defense Contractor MORSECORP Inc. Agrees to Pay $4.6 Million to Settle Cybersecurity Fraud Allegations

In January 2021, MORSE submitted to the Department of Defense a score of 104 for its implementation of the NIST SP 800-171 security controls. That score was near the top of the possible score range from -203 to 110. In July 2022, a third-party cybersecurity consultant notified MORSE that its score was actually -142. MORSE did not update its score in the Department of Defense reporting system until June 2023 — three months after the United States served MORSE with a subpoena concerning its cybersecurity practices.

Watson & Associates, LLC
Attorneys | Consultants

Cybersecurity Non-Compliance

Health Net Federal Services Inc. (HNFS) of Rancho Cordova, California and its corporate parent, St. Louis-based Centene Corporation, have agreed to pay $11,253,400 to resolve claims that HNFS falsely certified compliance with cybersecurity requirements in a contract with the U.S. Department of Defense (DoD) to administer the Defense Health Agency's (DHA) TRICARE health benefits program for servicemembers and their families.

HNFS failed to meet certain cybersecurity controls and falsely certified compliance with them in annual reports to DHA that were required under its contract to administer the TRICARE program.

Furthermore, the United States alleged HNFS ignored reports from third-party security auditors and its internal audit department of cybersecurity risks on HNFS' networks and systems related to asset management; access controls; configuration settings; firewalls; end-of-life hardware and software in use; patch management (i.e., installing critical security updates released by vendors to counter known threats); vulnerability scanning; and password policies.

Watson & Associates, LLC
Attorneys | Consultants

Cybersecurity Non-Compliance

Jardon and Howard Technologies, Inc., B-415330.3; B-415330.4

Jardon and Howard Technologies, Inc. (JHT), of Orlando, Florida, protests the establishment of a Federal Supply Schedule (FSS) blanket purchase agreement (BPA) with Consolidated Safety Services, Inc. (CSS), of Fairfax, Virginia, under request for quotations (RFQ) No. NCNS4000-17-00042, issued by the Department of Commerce, National Oceanic and Atmospheric Administration (NOAA), for scientific and technical mission support services.

Our [CSS] Corporate Security Plan defines procedures, responsibilities, and systems for maintaining physical and electronic security . . . . All on-site employees complete NOAA Cyber Security Awareness Training within five days of contract award, and comply with all security requirements as specified in the Solicitation.

Watson & Associates, LLC
Attorneys | Consultants

FAR 52.204-21

Covered contractor information system means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.

Federal contract information means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.

Information means any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

Watson & Associates, LLC
Attorneys | Consultants

FAR 52.204-21

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Safeguarding means measures or controls that are prescribed to protect information systems.

Watson & Associates, LLC
Attorneys | Consultants

Safeguarding requirements and procedures

(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

(iii) Verify and control/limit connections to and use of external information systems.

(iv) Control information posted or processed on publicly accessible information systems.

(v) Identify information system users, processes acting on behalf of users, or devices.

Watson & Associates, LLC
Attorneys | Consultants

Safeguarding requirements and procedures

(vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

(vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

(viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

(ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.

Watson & Associates, LLC
Attorneys | Consultants

Safeguarding requirements and procedures

(x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

(xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

(xii) Identify, report, and correct information and information system flaws in a timely manner.

Watson & Associates, LLC
Attorneys | Consultants

Safeguarding requirements and procedures

(xiii) Provide protection from malicious code at appropriate locations within organizational information systems.

(xiv) Update malicious code protection mechanisms when new releases are available.

(xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed

Watson & Associates, LLC
Attorneys | Consultants

DFARS 252.204-7012

"**Adequate security**" means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

"**Compromise**" means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

Watson & Associates, LLC
Attorneys | Consultants

DFARS 252.204-7012

Contractor attributional/proprietary information means information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.

Controlled technical information means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

Watson & Associates, LLC
Attorneys | Consultants

DFARS 252.204-7012

Covered contractor information system means an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.

Covered defense information means unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is—(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or (2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

Watson & Associates, LLC
Attorneys | Consultants

DFARS 252.204-7012

Cyber incident means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

Forensic analysis means the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Watson & Associates, LLC
Attorneys | Consultants

DFARS 252.204-7012

Malicious software means computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.

Media means physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which covered defense information is recorded, stored, or printed within a covered contractor information system.

Watson & Associates, LLC
Attorneys | Consultants

DFARS 252.204-7012

"Operationally critical support" means supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.

"Rapidly report" means within 72 hours of discovery of any cyber incident.

Watson & Associates, LLC
Attorneys | Consultants

DFARS 252.204-7012

"Technical information" means technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013 , *Rights in Technical Data—Other Than Commercial Products and Commercial Services*, regardless of whether or not the clause is incorporated in this solicitation or contract.

Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

Watson & Associates, LLC
Attorneys | Consultants

DFARS 252.204-7012

(b) Adequate security. The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:
(1) For covered contractor information systems that are part of an Information Technology (IT) service or system operated on behalf of the Government, the following security requirements apply:
(i) Cloud computing services shall be subject to the security requirements specified in the clause 252.239-7010, Cloud Computing Services, of this contract.
(ii) Any other such IT service or system (i.e., other than cloud computing) shall be subject to the security requirements specified elsewhere in this contract.

Watson & Associates, LLC
Attorneys | Consultants

DFARS 252.204-7012

(b) Adequate security (continued)

(2) For covered contractor information systems that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b)(1) of this clause, the following security requirements apply:
(i) Except as provided in paragraph (b)(2)(ii) of this clause, the covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations” (available via the internet at https://csrc.nist.gov/publications/sp800) in effect at the time the solicitation is issued or as authorized by the Contracting Officer.

…

Watson & Associates, LLC
Attorneys | Consultants

DFARS 252.204-7012

(b) Adequate security (continued)

(D) If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (https://www.fedramp.gov/documents-templates/) and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this clause for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.

…

Watson & Associates, LLC
Attorneys | Consultants

DFARS 252.204-7012

(b) Adequate security (continued)

(3) Apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraphs (b)(1) and (2) of this clause, may be required to provide adequate security in a dynamic environment or to accommodate special circumstances (e.g., medical devices) and any individual, isolated, or temporary deficiencies based on an assessed risk or vulnerability. These measures may be addressed in a system security plan….

Watson & Associates, LLC
Attorneys | Consultants

DFARS 252.204-7012

(c) Cyber incident reporting requirement.

(1) When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract, the Contractor shall—

(i) Conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor's network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Contractor's ability to provide operationally critical support; and

(ii) Rapidly report cyber incidents to DoD at https://dibnet.dod.mil.

Watson & Associates, LLC
Attorneys | Consultants

DFARS 252.204-7012

(h) DoD safeguarding and use of contractor attributional/proprietary information. The Government shall protect against the unauthorized use or release of information obtained from the contractor (or derived from information obtained from the contractor) under this clause that includes contractor attributional/proprietary information, including such information submitted in accordance with paragraph (c). To the maximum extent practicable, the Contractor shall identify and mark attributional/proprietary information. In making an authorized release of such information, the Government will implement appropriate procedures to minimize the contractor attributional/proprietary information that is included in such authorized release, seeking to include only that information that is necessary for the authorized purpose(s) for which the information is being released.

Watson & Associates, LLC
Attorneys | Consultants

DFARS 252.204-7012

(m) Subcontracts. The Contractor shall—

(1) Include this clause, including this paragraph (m), in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve covered defense information, including subcontracts for commercial products or commercial services, without alteration, except to identify the parties. The Contractor shall determine if the information required for subcontractor performance retains its identity as covered defense information and will require protection under this clause, and, if necessary, consult with the Contracting Officer; and

Watson & Associates, LLC
Attorneys | Consultants

DFARS 252.204-7012

(m) Subcontracts. The Contractor shall (continued) —

2) Require subcontractors to—

(i) Notify the prime Contractor (or next higher-tier subcontractor) when submitting a request to vary from a NIST SP 800-171 security requirement to the Contracting Officer, in accordance with paragraph (b)(2)(ii)(B) of this clause; and

(ii) Provide the incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable, when reporting a cyber incident to DoD as required in paragraph (c) of this clause.

Watson & Associates, LLC
Attorneys | Consultants

DFARS 252.239-7010

Spillage security incident that results in the transfer of classified or controlled unclassified information onto an information system not accredited (i.e., authorized) for the appropriate security level.

Cloud computing security requirements. The requirements of this clause are applicable when using cloud computing to provide information technology services in the performance of the contract.

(2) The Contractor shall implement and maintain administrative, technical, and physical safeguards and controls with the security level and services required in accordance with the Cloud Computing Security Requirements Guide (SRG) (version in effect at the time the solicitation is issued or as authorized by the Contracting Officer) found at https://public.cyber.mil/dccs/dccs-documents/ unless notified by the Contracting Officer that this requirement has been waived by the DoD Chief Information Officer.

Watson & Associates, LLC
Attorneys | Consultants

DFARS 252.239-7010

(g) Access to additional information or equipment necessary for forensic analysis. Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.

(h) Cyber incident damage assessment activities. If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph (f) of this clause.

Watson & Associates, LLC
Attorneys | Consultants

DFARS 252.239-7010

(j) *Notification of third party access requests.* The Contractor shall notify the Contracting Officer promptly of any requests from a third party for access to Government data or Government-related data, including any warrants, seizures, or subpoenas it receives, including those from another Federal, State, or local agency.
The Contractor shall cooperate with the Contracting Officer to take all measures to protect Government data and Government-related data from any unauthorized disclosure.
(k) *Spillage.* Upon notification by the Government of a spillage, or upon the Contractor's discovery of a spillage, the Contractor shall cooperate with the Contracting Officer to address the spillage in compliance with agency procedures.
(l) *Subcontracts*. The Contractor shall include this clause, including this paragraph (l), in all subcontracts that involve or may involve cloud services, including subcontracts for commercial services.

Watson & Associates, LLC
Attorneys | Consultants

DFARS 252.204-7009

(b) Restrictions. The Contractor agrees that the following conditions apply to any information it receives or creates in the performance of this contract that is information obtained from a third-party's reporting of a cyber incident pursuant to DFARS clause 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting* (or derived from such information obtained under that clause):

Watson & Associates, LLC
Attorneys | Consultants

DFARS 252.204-7009

(b) Restrictions (continued)

(1) The Contractor shall access and use the information only for the purpose of furnishing advice or technical assistance directly to the Government in support of the Government's activities related to clause 252.204-7012, and shall not be used for any other purpose.
(2) The Contractor shall protect the information against unauthorized release or disclosure.
(3) The Contractor shall ensure that its employees are subject to use and nondisclosure obligations consistent with this clause prior to the employees being provided access to or use of the information.
(4) The third-party contractor that reported the cyber incident is a third-party beneficiary of the nondisclosure agreement between the Government and Contractor, as required by paragraph (b)(3) of this clause.

Watson & Associates, LLC
Attorneys | Consultants

DFARS 252.204-7009

(b) Restrictions (continued)

(5) A breach of these obligations or restrictions may subject the Contractor to—

(i) Criminal, civil, administrative, and contractual actions in law and equity for penalties, damages, and other appropriate remedies by the United States; and

(ii) Civil actions for damages and other appropriate remedies by the third party that reported the cyber incident, as a third party beneficiary of this clause.

Watson & Associates, LLC
Attorneys | Consultants

DFARS 252.204-7009

(b) Restrictions (continued)

(c) Subcontracts. The Contractor shall include this clause, including this paragraph (c), in subcontracts, or similar contractual instruments, for services that include support for the Government's activities related to safeguarding covered defense information and cyber incident reporting, including subcontracts for commercial items, without alteration, except to identify the parties.

Watson & Associates, LLC
Attorneys | Consultants

Cybersecurity

Most Common Risks

Ransomware	Malicious Code	Destructive Malware
Spyware	Denial of Access Attacks	Phishing
Imposters	Wireless Networks	Website Security
Cell Phones	Travel	Anything Else?

Watson & Associates, LLC
Attorneys | Consultants

Cybersecurity Best Practices

Best Practices

CSF functions and categories

Function	Purpose	Categories
Identify	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.	Asset Management, Business Environment, Governance, Risk Assessment, Risk Management Strategy, Supply Chain Risk Management
Protect	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.	Identity Management, Authentication and Access Control, Awareness & Training, Data Security, Info Protection and Procedures, Maintenance, Protective Technology
Detect	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.	Anomalies and Events, Security Continuous Monitoring, Detection Process
Respond	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.	Response Planning, Communications, Analysis, Mitigation, Improvements
Recover	Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.	Recovery Planning, Improvements, Communications

Access Control, Configuration Management, Incident Response, and Audit Logs

Watson & Associates, LLC
Attorneys | Consultants

Cybersecurity Best Practices

Best Practices

Multi-Factor Authentication

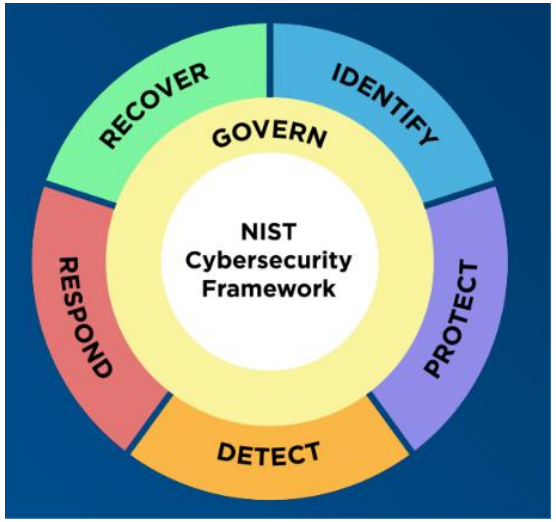
Reliable Encryption

Vulnerability Scanning on Daily Basis

Zero Trust Architecture

Remote Access/Individual Access/Information Access Limitations

Sub-Contractor Flowdown



Not Legal Advice / For Educational Purposes Only

Watson & Associates, LLC
Attorneys | Consultants

Cybersecurity Best Practices

Best Practices

Strong Passwords

Current Software

Training

Cybersecurity Response and Reporting Drills

Monitor Compliance

Reduce Connectivity

Incident Planning

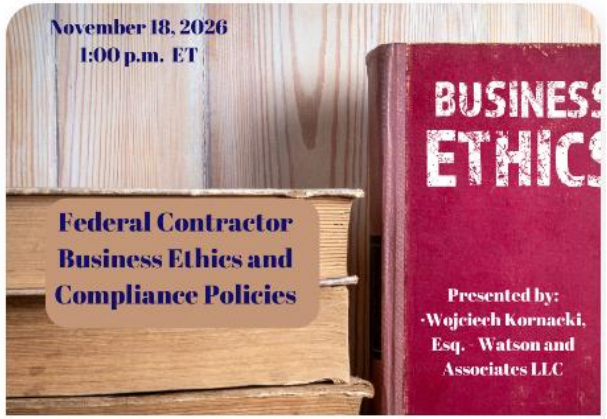
Additional Courses:

2026-07-30

2026-08-27

2026-09-28

2026-10-29



2026-11-18

2026-12-10

Not Legal Advice / For Educational Purposes Only

Thank you!

Wojciech Kornacki
Government Contract and Compliance Counsel,
Of Counsel
kornackiw@theodorewatson.com I 202.640-3023

CRITICAL THINKING, CLEAR DIRECTION, DECISIVE RESULTS

Not Legal Advice / For Educational Purposes Only

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

Presidential Documents

Title 3—

The President

Executive Order 13556 of November 4, 2010

Controlled Unclassified Information

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

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

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

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

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

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

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

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

Sec. 3. *Review of Current Designations.*

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

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

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

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

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

(a) On the basis of the submissions under section 3 of this order or future proposals, and in consultation with affected agencies, the Executive Agent shall, in a timely manner, approve categories and subcategories of CUI and associated markings to be applied uniformly throughout the executive branch and to become effective upon publication in the registry established under subsection (d) of this section. No unclassified information meeting the requirements of section 2(a) of this order shall be disapproved for inclusion as CUI, but the Executive Agent may resolve conflicts among categories and subcategories of CUI to achieve uniformity and may determine the markings to be used.

(b) The Executive Agent, in consultation with affected agencies, shall develop and issue such directives as are necessary to implement this order. Such directives shall be made available to the public and shall provide policies and procedures concerning marking, safeguarding, dissemination, and decontrol of CUI that, to the extent practicable and permitted by law, regulation, and Government-wide policies, shall remain consistent across categories and subcategories of CUI and throughout the executive branch. In developing such directives, appropriate consideration should be given to the report of the interagency Task Force on Controlled Unclassified Information published in August 2009. The Executive Agent shall issue initial directives for the implementation of this order within 180 days of the date of this order.

(c) The Executive Agent shall convene and chair interagency meetings to discuss matters pertaining to the program established by this order.

(d) Within 1 year of the date of this order, the Executive Agent shall establish and maintain a public CUI registry reflecting authorized CUI categories and subcategories, associated markings, and applicable safeguarding, dissemination, and decontrol procedures.

(e) If the Executive Agent and an agency cannot reach agreement on an issue related to the implementation of this order, that issue may be appealed to the President through the Director of the Office of Management and Budget.

(f) In performing its functions under this order, the Executive Agent, in accordance with applicable law, shall consult with representatives of the public and State, local, tribal, and private sector partners on matters related to approving categories and subcategories of CUI and developing implementing directives issued by the Executive Agent pursuant to this order.

Sec. 5. *Implementation.*

(a) Within 180 days of the issuance of initial policies and procedures by the Executive Agent in accordance with section 4(b) of this order, each agency that originates or handles CUI shall provide the Executive Agent with a proposed plan for compliance with the requirements of this order, including the establishment of interim target dates.

(b) After a review of agency plans, and in consultation with affected agencies and the Office of Management and Budget, the Executive Agent shall establish deadlines for phased implementation by agencies.

(c) In each of the first 5 years following the date of this order and biennially thereafter, the Executive Agent shall publish a report on the status of agency implementation of this order.

Sec. 6. *General Provisions.*

(a) This order shall be implemented in a manner consistent with:

(1) applicable law, including protections of confidentiality and privacy rights;

(2) the statutory authority of the heads of agencies, including authorities related to the protection of information provided by the private sector to the Federal Government; and

(3) applicable Government-wide standards and guidelines issued by the National Institute of Standards and Technology, and applicable policies established by the Office of Management and Budget.

(b) The Director of National Intelligence (Director), with respect to the Intelligence Community and after consultation with the heads of affected agencies, may issue such policy directives and guidelines as the Director deems necessary to implement this order with respect to intelligence and intelligence-related information. Procedures or other guidance issued by Intelligence Community element heads shall be in accordance with such policy directives or guidelines issued by the Director. Any such policy directives or guidelines issued by the Director shall be in accordance with this order and directives issued by the Executive Agent.

(c) This order shall not be construed to impair or otherwise affect the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, and legislative proposals.

(d) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

(e) This order shall be implemented subject to the availability of appropriations.

(f) The Attorney General, upon request by the head of an agency or the Executive Agent, shall render an interpretation of this order with respect to any question arising in the course of its administration.

(g) The Presidential Memorandum of May 7, 2008, entitled "Designation and Sharing of Controlled Unclassified Information (CUI)" is hereby rescinded.

THE WHITE HOUSE,
November 4, 2010.

[FR Doc. 2010–28360
Filed 11–8–10; 8:45 am]
Billing code 3195–W1–P

DoD Instruction 5200.48

Controlled Unclassified Information (CUI)

Originating Component:	Office of the Under Secretary of Defense for Intelligence and Security
Effective:	March 6, 2020
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Cancels:	DoD Manual 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information," February 24, 2012, as amended
Approved by:	Joseph D. Kernan, Under Secretary of Defense for Intelligence and Security (USD(I&S))

Purpose: In accordance with the authority in DoD Directive (DoDD) 5143.01 and the December 22, 2010 Deputy Secretary of Defense Memorandum, this issuance:

- Establishes policy, assigns responsibilities, and prescribes procedures for CUI throughout the DoD in accordance with Executive Order (E.O.) 13556; Part 2002 of Title 32, Code of Federal Regulations (CFR); and Defense Federal Acquisition Regulation Supplement (DFARS) Sections 252.204-7008 and 252.204-7012.
- Establishes the official DoD CUI Registry.

TABLE OF CONTENTS

TABLES

FIGURES

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

This issuance applies to:

a. Office of the Secretary of Defense (OSD), the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense (OIG DoD), the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this issuance as the "DoD Components").

b. Arrangements, agreements, contracts, and other transaction authority actions requiring access to CUI according to terms and conditions of such documents, as defined in Clause 2.101 of the Federal Acquisition Regulation and Section 2002.4 of Title 32, CFR, including, but not limited to, grants, licenses, certificates, memoranda of agreement/arrangement or understanding, and information-sharing agreements or arrangements.

1.2. POLICY.

It is DoD policy that:

a. As part of the phased DoD CUI Program implementation process endorsed by the CUI Executive Agent (EA) pursuant to Information Security Oversight Office (ISOO) Memorandum dated August 21, 2019, the designation, handling, and decontrolling of CUI (including CUI identification, sharing, marking, safeguarding, storage, dissemination, destruction, and records management) will be conducted in accordance with this issuance and Sections 252.204-7008 and 252.204-7012 of the DFARS when applied by a contract to non-DoD systems.

b. All DoD CUI must be controlled until authorized for public release in accordance with DoD Instructions (DoDIs) 5230.09, 5230.29, and 5400.04, or DoD Manual (DoDM) 5400.07. Official DoD information that is not classified or controlled as CUI will also be reviewed prior to public release in accordance with DoDIs 5230.09 or5230.29.

c. Information will not be designated CUI in order to:

(1) Conceal violations of law, inefficiency, or administrative error.

(2) Prevent embarrassment to a person, organization, or agency.

(3) Prevent open competition.

(4) Control information not requiring protection under a law, regulation, or government-wide policy, unless approved by the CUI EA at the National Archives and Records Administration (NARA), through the Under Secretary of Defense for Intelligence and Security (USD(I&S)).

d. In accordance with the DoD phased CUI Program implementation, all documents containing CUI must carry CUI markings in accordance with this issuance.

e. Although DoD Components are not required to use the terms “Basic” or “Specified” to characterize CUI at this time, DoD Components will apply:

(1) At least the minimum safeguards required to protect CUI.

(2) Terms and specific marking requirements will be promulgated by the USD(I&S) in future guidance.

f. Nothing in this issuance alters or supersedes the existing authorities of the Director of National Intelligence (DNI) regarding CUI.

g. Nothing in this issuance will infringe on the OIG DoD’s statutory independence and authority, as articulated in the Inspector General Act of 1978 in the Title 5, United States Code (U.S.C.) Appendix. In the event of any conflict between this instruction and the OIG DoD’s statutory independence and authority, the Inspector General Act of 1978 in the Title 5, U.S.C. Appendix takes precedence.

SECTION 2: RESPONSIBILITIES

2.1. USD(I&S)

The USD(I&S):

a. As the DoD Senior Agency Official for Security, establishes policy and oversees the DoD Information Security Program.

b. In coordination with the requesting DoD Component, submits changes to CUI categories on behalf of DoD Components to the CUI EA at NARA.

c. Provides reports to the CUI EA on the DoD CUI Program status, as described in Paragraph 3.6.c., in accordance with Part 2002 of Title 32, CFR.

d. Establishes protocol for resolving disputes about implementing or interpreting E.O. 13556, Part 2002 of Title 32, CFR, the CUI Registry, and this issuance, within and between the DoD Components.

e. Coordinates with the Department of Defense Chief Information Officer (DoD CIO) on CUI waiver requests for DoD information systems (IS) and networks.

f. Coordinates with the CUI EA on DoD Component CUI waiver requests.

2.2. DIRECTOR FOR DEFENSE INTELLIGENCE (COUNTERINTELLIGENCE, LAW ENFORCEMENT, AND SECURITY (DDI(CL&S)).

The DDI(CL&S):

a. Oversees and manages the DoD CUI Program.

b. Reviews and signs all reports and other correspondence related to the DoD CUI Program.

c. Coordinates with the Secretaries of the Military Departments, Under Secretary of Defense for Research and Engineering (USD(R&E)), Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)), and the DoD Component heads to:

(1) Recommend changes to national CUI policy relating to identifying, safeguarding, disseminating, marking, storing, transmitting, reviewing, transporting, re-using, decontrolling, and destroying CUI, and responding to unauthorized disclosure (UD) of CUI.

(2) Review and provide guidance on DoD Component implementation policy and CUI-related matters.

d. Assists the USD(I&S) with overseeing the CUI policy and program execution via the Defense Security Enterprise Executive Committee in accordance with DoDD 5200.43.

e. In coordination with the DoD CIO, USD(A&S), and USD(R&E), provides guidance on implementing uniform standards to display TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED for CNSI and CUI controls and banners for DoD systems and networks.

2.3. DIRECTOR, DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY (DSCA).

Under the authority, direction, and control of the USD(I&S) and in addition to the responsibilities in Paragraph 2.10., the Director, DCSA:

a. Administers the DoD CUI Program for contractually established CUI requirements for contractors in classified contracts in accordance with the May 17, 2018 Under Secretary of Defense for Intelligence Memorandum.

b. Assesses contractor compliance with contractually established CUI system requirements in DoD classified contracts associated with the National Industrial Security Program (NISP) in accordance with Part 2003 of Title 32, CFR and National Institute of Standards and Technology Special Publication (NIST SP) 800-171 guidelines.

c. Establishes and maintains a process to notify the DoD CIO, USD(R&E), and USD(A&S) of threats related to CUI for further dissemination to DoD Components and contractors in accordance with the Section 252.204-7012 of the DFARS.

d. Provides, in coordination with the USD(I&S), security education, training, and awareness on the required topics identified in Section 2002.30 of Title 32, CFR, including protection and management of CUI, to DoD personnel and contractors through the Center for Development of Security Excellence (CDSE).

e. Provides security assistance and guidance to the DoD Components on the protection of CUI when DoD Components establish CUI requirements in DoD classified contracts for NISP contractors falling under DCSA security oversight.

f. Serves as the DoD-lead to report UDs of CUI, except for the reporting of cyber incidents in accordance with Section 252.204-7012 of the DFARS, associated with contractually established CUI system requirements in DoD classified contracts for NISP contractors falling under DCSA security oversight.

g. Coordinates with the DoD CIO to implement uniform security requirements when the IS or network security controls for unclassified and classified information are included in DoD classified contracts for NISP contractors falling under DCSA security oversight.

h. Consolidates DoD Component input on the oversight of CUI protection requirements in DoD classified contracts for NISP contractors under DCSA security oversight, as required by Information Security Oversight Office (ISOO) Notice 2016-01.

2.4. CHIEF MANAGEMENT OFFICER OF THE DEPARTMENT OF DEFENSE (CMO).

In addition to the responsibilities in Paragraph 2.10., the CMO:

a. Serves as the subject matter expert on CUI containing personally identifiable information and its release in accordance with Subsection 552 of Chapter 5 of Title 5, United States Code (U.S.C.), also known as and referred to in this issuance as the "Freedom of Information Act (FOIA)," implemented through DoDD 5400.07 and DoDI 5400.11, and Subsection 552a of Chapter 5 of Title 5, U.S.C., also known and referred to in the issuance as the "Privacy Act of 1974."

b. Supports OSD with information security matters, as appropriate.

2.5. PFPA.

Under the authority, direction, and control of the CMO, through the Director for Administration and Organizational Policy, and in addition to the responsibilities in Paragraph 2.10., the Director, PFPA:

a. Provides information security administrative support to OSD.

b. Provides information on OSD CUI Program status and other formally requested assistance to the USD(I&S) to support the CUI Program.

c. Conducts CUI staff assistance visits to OSD in the National Capital Region.

2.6. UNDER SECRETARY OF DEFENSE FOR POLICY.

In addition to the responsibilities in Paragraph 2.10., the Under Secretary of Defense for Policy:

a. Establishes policy and procedures for disclosing DoD CUI to foreign governments, the North Atlantic Treaty Organization, and international organizations based on formally signed agreements and arrangements between the parties.

b. Requires CUI to be identified in international agreements, arrangements, and contracts having licensing export controls for foreign partners.

2.7. USD(A&S).

In addition to the responsibilities in Paragraph 2.10., pursuant to Section 133b of Title 10, U.S.C., and in coordination with the USD(I&S), DoD CIO, and USD(R&E), the USD(A&S):

a. Maintains, in accordance with Section 252.204-7012 of the DFARS, DoD acquisition contracting processes, policies, and procedures for safeguarding DoD CUI in DoD procurement arrangements, agreements, and contracts, including other transaction authority actions.

b. Supports the development and implementation of a Federal Acquisition Regulation clause applying CUI requirements to defense contractors.

2.8. USD(R&E).

In addition to the responsibilities in Paragraph 2.10., pursuant to Section 133a of Title 10, U.S.C., and in coordination with USD(I&S), the USD(R&E):

a. Establishes DoD CUI processes, policies, and procedures for grants and cooperative research and development arrangements, agreements, and contracts involving controlled technical information (CTI).

b. Establishes a standard process to identify CTI; guidelines for sharing, marking, safeguarding, storing, disseminating, decontrolling, and destroying CTI; and CTI records management requirements contained in contracts, as appropriate.

c. Oversees and ensures DoD CUI guidelines and requirements for sharing, marking, safeguarding, storage, dissemination, decontrol, destruction, and records management of all research, development, test, and evaluation information are properly executed for all DoD owned records.

d. In coordination with the USD(A&S), ensures:

(1) Contracts, arrangements, and agreements for research, development, testing, and evaluation identify CUI at the time of award.

(2) USD(R&E) international agreements, arrangements, and contracts with foreign partners identify CUI within the documents.

(3) DoD Components concluding international agreements, arrangements, and contracts with foreign partners include U.S. Government-approved text on CUI.

2.9. DOD CIO.

In addition to the responsibilities in Paragraph 2.10., the DoD CIO:

a. Oversees CUI metadata tagging standards, consistent with federal data tagging approaches in accordance with the National Strategy for Information Sharing and Safeguarding, to implement the marking requirements in Paragraph 3.4.c. and in accordance with DoDI 8320.07.

b. Integrates CUI metadata tagging standards into DoD information technology content management tools to support discovery, access, auditing, safeguarding, and records management decisions regarding CUI (including monitoring CUI data for visibility, accessibility, trust, interoperability, and comprehension).

c. Provides policy and standards recommendations to the USD(I&S) on updates for the sharing, marking, safeguarding, storage, dissemination, decontrol, destruction, and records

management of DoD CUI residing on both DoD and non-DoD IS in accordance with DoDI 8582.01.

d. Oversees Defense Industrial Base Cybersecurity Activities, using the DoD Cyber Crime Center as the single DoD focal point for receiving and disseminating all cyber incident reports impacting unclassified networks of defense contractors.

e. Coordinates with the USD(I&S), USD(A&S), USD(R&E), and DoD Component heads to develop uniform security requirements for industry partners' IS and network security controls adequate for the type of CUI identified in the contract in accordance with Part 2002 of Title 32, CFR, Section 252.204-7012 of the DFARS, and NIST SP 800-171.

f. Coordinates with the Director, DCSA to implement uniform security requirements when IS or network security controls for unclassified and classified information are included in DoD classified contracts of NISP contractors falling under DCSA security oversight.

g. Coordinates with the USD(I&S) to:

(1) Implement information security policy standards for markings to display, CUI for DoD classified and unclassified systems and networks.

(2) Integrate training on safeguarding and handling CUI into updates to initial and annual cybersecurity awareness training.

h. Notifies the CUI EA in coordination with the USD(I&S) of CUI waivers impacting IS or networks in accordance with Title 32 of the CFR.

i. Oversees and ensures DoD Component- and National Archives-approved disposition authorities for CUI are implemented for DoD records and information.

j. Oversees and ensures the Director, DoD Cyber Crime Center:

(1) Manages and updates, as necessary and in coordination with DoD CIO, the policies in Section 236.4 of Title 32, CFR and Section 252.204-7012 of the DFARS.

(2) Maintains the website at https://dibnet.dod.mil to receive contractor mandatory incident reports in accordance with Paragraph 3.9.d(1).

2.10. OSD AND DOD COMPONENT HEADS.

OSD and DoD Component heads:

a. Identify, program, and commit the necessary resources to implement CUI Program requirements as part of their overall information security programs.

b. Designate in writing (with copy to the USD(I&S)):

(1) A DoD Component senior agency official (CSAO) at the Senior Executive Service level or equivalent to implement their CUI Program and perform the duties in Paragraph 3.5.

(2) A DoD Component program manager (CPM) to manage their CUI Program.

c. Ensure their subordinate organizations comply with DoD CUI Program requirements.

d. Ensure their personnel receive initial and annual refresher CUI education and training, and maintain documentation of this training for audit purposes.

e. Report DoD Component training completion data to the USD(I&S) annually or as directed.

f. Provide an annual report to the USD(I&S) on CUI implementation status in accordance with Title 32, CFR, Part 2002.

g. Determine if any CUI documents or materials constitute permanently valuable records of the government, which require maintenance and disposal in accordance with DoDI 5015.02.

h. As the requiring activity, oversee CUI requirements for contractor implementation in partnership with the Defense Contract Management Agency, based on Defense Contract Management Agency responsibilities, or DCSA for cleared contractors in accordance with the NISP, as appropriate.

i. Ensure DoD Component- and National Archives-approved disposition authorities are implemented for DoD records and information regardless of classification.

j. Manage their CUI programs in accordance with guidelines prescribed in this DoD issuance.

2.11. SECRETARIES OF THE MILITARY DEPARTMENTS.

In addition to the responsibilities in Paragraph 2.10., the Secretaries of the Military Departments oversee the implementation of their CUI programs.

2.12. CHAIRMAN OF THE JOINT CHIEFS OF STAFF.

In addition to the responsibilities in Paragraph 2.10., the Chairman of the Joint Chiefs of Staff oversees the implementation of the CUI programs in the Joint Staff organizations and Combatant Commands.

SECTION 3: PROGRAMMATICS

3.1. BACKGROUND.

The CUI EA at NARA, through the Information Security and Oversight Office (ISOO), published and released Part 2002 of Title 32, CFR, which provides implementing requirements for E.O. 13556.

a. Part 2002 of Title 32, CFR established a CUI EA office under NARA's ISOO for implementing and overseeing the CUI Program.

b. Designed as a response to the information sharing challenges from inconsistent definitions and marking requirements applied to CUI, Part 2002 of Title 32 CFR standardized the definition of CUI and codified the identification, sharing, safeguarding, marking, storage, distribution, transmission, decontrol, destruction, training, monitoring, and reporting requirements across the Executive branch of government.

c. In accordance with Part 2002 of Title 32, CFR, CUI requires safeguarding or dissemination controls identified in a law, regulation, or government-wide policy for information that does not meet the requirements for classification in accordance with E.O. 13526.

d. Unlike classified information, an individual or organization generally does not need to demonstrate a need-to-know to access CUI, unless required by a law, regulation, or government-wide policy, but must have a lawful governmental purpose for such access. One example of a requirement for need-to-know established by law, regulation, or government-wide policy is Section 223.6 of Title 32, CFR, which requires a person to have a need-to-know to be granted access to DoD Unclassified Nuclear Information (UCNI).

3.2. LEGACY INFORMATION REQUIREMENTS.

This legacy information guidance applies to information contained across DoD in, among other documents, security classification guides (SCGs), various policies, and other legacy materials falling under the Science and Technology Information Program (DoDI 3200.12), in either electronic or hardcopy format. The CUI Program does not require the redacting or re-marking of documents bearing legacy markings. However, any new document created with information derived from legacy material must be marked as CUI if the information qualifies as CUI.

a. DoD legacy material will not be required to be re-marked or redacted while it remains under DoD control or is accessed online and downloaded for use within the DoD. However, any such document or new derivative document must be marked as CUI if the information qualifies as CUI and the document is being shared outside DoD. DoD legacy marked information stored on a DoD access-controlled website or database does not need to be remarked as CUI, even if other agencies and contractors are granted access to such websites or databases.

b. DoD legacy information does not automatically become CUI. It must be reviewed by the owner of the information to determine if it meets the CUI requirements. If it is determined the

specific legacy information meets the CUI requirements, it will be marked in accordance with this issuance and corresponding manual.

c. For federal systems, IS storing information identified as CUI must meet the minimum network security standard in Part 2002 of Title 32, CFR. For nonfederal systems, IS must meet the standards in the NIST SP 800-171, when established by contract.

d. When DoD legacy information is incorporated into, or cited in, another document or material, it must be reviewed for CUI and marked in accordance with this issuance.

3.3. HANDLING REQUIREMENTS.

The DoD CUI Information Security Program will promote, to the maximum extent possible, information sharing, facilitate informed resource use, and simplify its management and implementation while maintaining required safeguarding and handling measures.

a. In accordance with DoDI 5230.09 and the August 14, 2014 Deputy Secretary of Defense Memorandum:

(1) The DoD originator or authorized CUI holder must ensure a prepublication and security policy review is conducted, pursuant to the standard DoD Component process, before CUI is approved for public release, which includes publication to a publicly accessible website.

(2) Decontrolling and releasing CUI records will be executed by the originator of the information, the original classification authority (OCA) if identified in a security classification guide, or designated offices for decontrolling CUI pursuant to the procedures for the review and release of information under the FOIA in accordance with the November 19, 2018 ISOO Notice. There are no specific timelines to decontrol CUI unless specifically required in a law, regulation, or government-wide policy. Decontrol will occur when the CUI no longer requires safeguarding and will follow DoD records management procedures.

b. OCAs will determine if aggregated CUI under their control should be classified in accordance with Volume 1 of DoDM 5200.01 and will confirm the relevant SCGs address the compilation.

c. DoD information systems processing, storing, or transmitting CUI will be categorized at the “moderate” confidentiality impact level and follow the guidance in DoDIs 8500.01 and 8510.01. Non-DoD information systems processing, storing, or transmitting CUI will provide adequate security, and the appropriate requirements must be incorporated into all contracts, grants, and other legal agreements with non-DoD entities in accordance with DoDI 8582.01. See Section 5 of this issuance for more information on CUI and its application to industry.

d. The DoD CUI Registry provides an official list of the Indexes and Categories used to identify the various types of DoD CUI. The DoD CUI Registry mirrors the National CUI Registry, but provides additional information on the relationships to DoD by aligning each Index and Category to DoD issuances.

(1) The official DoD CUI Registry of categories can be accessed on Intelink at https://intelshare.intelink.gov/sites/ousdi/hcis/sec/icdirect/information/CUI/Forms/AllItems.aspx.

(2) The site will be updated as changes to the DoD CUI Registry are made based on official notification from the CUI EA through the CUI Registry Working Group; changes to law, regulation, or government-wide policy; or notification that the information no longer meets the requirements for CUI.

3.4. MARKING REQUIREMENTS.

This paragraph covers the essential marking requirements for initial phased implementation of the DoD CUI Program.

a. At minimum, CUI markings for unclassified DoD documents will include the acronym "CUI" in the banner and footer of the document.

b. If portion markings are selected, then all document subjects and titles, as well as individual sections, parts, paragraphs, or similar portions of a CUI document known to contain CUI, will be portion marked with "(CUI)." Use of the unclassified marking "(U)" as a portion marking for unclassified information within CUI documents or materials is required.

(1) There is no requirement to add the "U," signifying unclassified, to the banner and footer as was required with the old FOUO marking (i.e., U//FOUO).

(2) Banners, footers, and portion marking will only be marked "Unclassified" or "(U)" for unclassified information in accordance with the June 4, 2019 ISOO letter. If the document also contains CUI, it will be marked in accordance with Paragraph 3.4.a. and additional forthcoming guidance.

c. CUI markings in classified documents will appear in paragraphs or subparagraphs known to contain **only** CUI and must be portion marked with "(CUI)." "CUI" will **not** appear in the banner or footer.

(1) There will be an acknowledgement added to the warning box on the first page of multi-page documents to alert readers to the presence of CUI in a classified DoD document, as shown in Figure 1.

Figure 1. CUI Warning Box for Classified Material

This content is classified at the [insert highest classification level of the source data] level and may contain elements of controlled unclassified information (CUI), unclassified, or information classified at a lower level than the overall classification displayed. This content shall not be used as a source of derivative classification; refer instead to [cite specific reference, where possible, or state "the applicable classification guide(s)"]. It must be reviewed for both Classified National Security Information (CNSI) and CUI in accordance with DoDI 5230.09 prior to public release. [Add a point of contact when needed.]

(2) Volume 2 of DoDM 5200.01 requires DoD intelligence producers to follow DNI formats for intelligence production under the authority of the DNI. When DoD CUI is incorporated into a Digital Access Policy under the authority of the DNI, the information and the document will follow the Digital Access Policy standards established by the DNI.

d. The dissemination marking "not releasable to foreign nationals (NOFORN or NF)" is an intelligence control marking used to identify intelligence information an originator has determined meets the criteria of Intelligence Community Directive 710 and Intelligence Community Policy Guidance 403.1, which provides guidance for further dissemination control markings. It must be applied to controlled unclassified intelligence information that is properly characterized as CUI with appropriate CUI markings. CUI identified with this marking will not be provided, in any form, to foreign governments (including coalition partners), international organizations, foreign nationals, or other non-U.S. persons without the originator's approval in accordance with E.O.s 13526 and 13556. If originator approval is required for further dissemination, the originator will mark the requirement on the information in accordance with Section 4.1(i)(1) of E.O. 13526.

(1) The application of the control marking "not releasable to foreign nationals" (NOFORN or NF) will only be applied, when warranted, to unclassified intelligence information properly categorized as CUI and reviewed by a Foreign Disclosure Officer to ensure there are no international agreements in place to prohibit its use and prohibiting sharing.

(2) The control marking NOFORN or NF will be applied to Naval Nuclear Propulsion Information (NNPI), Unclassified Controlled Nuclear Information (UCNI), National Disclosure Policy (NDP-1), and cover and cover support information. When warranted, it can be applied to unclassified information properly categorized as CUI having a licensing or export control requirement. Before marking a document or material as NOFORN or NF, it will be reviewed by the Foreign Disclosure Officer to ensure there are no agreements in place to prohibit its use and sharing.

(3) The application of "Releasable to" ("REL TO") can only be applied, when warranted and consistent with relevant law, regulation, or government-wide policy or DoD policy, to information properly categorized as CUI with an export control or licensing requirement with a foreign disclosure agreement in place.

(a) Export-controlled CUI transfers to foreign persons must be in accordance with the Arms Export Control Act, International Traffic in Arms Regulations, Export Control Reform Act, Export Administration Regulations, and DoDI 2040.02. In accordance with DoDDs 5230.11 and 5230.20, a positive foreign disclosure decision must be made before CUI is released to a foreign entity.

(b) DoD operational CUI (not related to intelligence) may be marked as REL TO.

e. All classified documents, including legacy documents will be reviewed for CUI and properly marked upon changes in the document's classification level, particularly if the documents are to be completely declassified.

f. The first page or cover of any document or material containing CUI, including a document with commingled classified information, will include a CUI designation indicator, as shown in Figure 2. This CUI designation indicator is similar to the classification-marking block used for CNSI documents and materials. Documents and materials containing CUI will require a generic "CUI" marking at the top and bottom of each page.

(1) In accordance with Part 2002 of Title 32, CFR, the CUI designation indicator must contain, at minimum, the name of the DoD Component determining that the information is CUI. If letterhead or another standard indicator of origination is used, this line may be omitted.

(2) The second line must identify the office making the determination.

(3) The third line must identify all types of CUI contained in the document.

(4) The fourth line must contain the distribution statement or the dissemination controls applicable to the document.

(5) The fifth line must contain the phone number or office mailbox for the originating DoD Component or authorized CUI holder.

Figure 2. CUI Designation Indicator for All Documents and Material

Controlled by: [Name of DoD Component] (Only if not on letterhead)
Controlled by: [Name of Office]
CUI Category: (List category or categories of CUI)
Distribution/Dissemination Control:
POC: [Phone or email address]

g. During DoD's initial phased implementation of the CUI Program, there is no required distinction that must be made between Basic and Specified CUI. All DoD information will be protected in accordance with the requirements under the Basic level of safeguards and dissemination unless specifically identified otherwise in a law, regulation, or government-wide policy. Forthcoming guidance will address the distinction between the two levels of CUI, including a list of which categories are Basic or Specified, what makes the category one or the other, and the unique requirements, to include markings, for each.

3.5. GENERAL DOD CUI ADMINISTRATIVE REQUIREMENTS.

Each DoD Component head must appoint, in writing, a CSAO for the Information Security Program, who will:

a. Appoint, in writing, an official to serve as the CPM for CUI in accordance with ISSO Notice 2019-02. To manage the DoD Component's overall execution of the CUI program, the CPM will:

(1) Coordinate directly with the USD(I&S) Information Security Directorate on CUI matters.

(2) Manage and oversee CUI implementation for the DoD Component.

(3) Inform the CSAO of concerns identified by subordinate elements.

(4) Report misuse, mishandling, or UD of CUI to the Unauthorized Disclosure Program Management Office. In addition, notify the appropriate Military Department Counterintelligence Organization of all incidents.

(5) Submit the annual CUI Implementation Status Report to the DDI(CL&S) to evaluate the effectiveness, compliance, and efficiency of the DoD Component's implementation of CUI, in accordance with Paragraph 3.6.c.

(6) Resolve CUI challenges in accordance with E.O. 13556 and Part 2002 of Title 32, CFR. Refer all unresolved challenges to the DDI(CL&S).

b. Serve as the primary point of contact for official correspondence, accountability reporting, and other matters of record between the DoD Component and the USD(I&S).

3.6. GENERAL DOD CUI PROCEDURES.

DoD CUI is clustered into organizational indexes (e.g., defense, privacy, proprietary) with associated categories, and is categorized by the DoD according to the specific law, regulation, or government-wide policy requiring control. Unclassified information associated with a law, regulation, or government-wide policy and identified as needing safeguarding is considered CUI. It requires access control, handling, marking, dissemination controls, and other protective measures for safeguarding.

a. The authorized holder of a document or material is responsible for determining, at the time of creation, whether information in a document or material falls into a CUI category. If so, the authorized holder is responsible for applying CUI markings and dissemination instructions accordingly.

b. In accordance with this issuance, every individual at every level, including DoD civilian and military personnel as well as contractors providing support to the DoD pursuant to

contractual requirements, will comply with the requirements in Paragraph 3.6.f of this issuance for initial and annual refresher CUI training.

c. Each OSD and DoD Component will annually submit the CUI Implementation Status Report to the USD(I&S) for inclusion in the DoD CUI Program report to the CUI EA. A copy of the report will be made available on Intelink at https://intelshare.intelink.gov/sites/ousdi/hcis/sec/icdirect/information/CUI/Forms/AllItems.aspx. The CUI Implementation Status Report will at least include:

(1) Implementation activities.

(2) Training statistics.

(3) Incident management.

(4) Implementation and sustainment costs.

(5) Self-inspection activities.

d. DoD and OSD Components will submit an initial report on the implementation status of their CUI Programs. Once established, DoD Component heads will conduct inspections of their programs, and the DoD Implementation Status Report will transition to an annual self-inspection report.

e. Some documents and materials containing CUI may constitute permanently valuable government records and will be maintained and disposed of in accordance with the NARA-approved record disposition schedules applicable to each DoD Component in accordance with DoDI 5015.02. When other materials containing CUI no longer require safeguarding, they will be decontrolled and either retained, if a permanent record, or destroyed in accordance with Section 4 and ISOO Notice 2019-03.

f. Other Executive Branch Agencies in the U.S. Government have identified organizational indexes and CUI categories related to a law, regulation, or government-wide policy. Some CUI indexes and categories are unique to specific organizations. The Official CUI Registry is on the NARA Website at https://www.archives.gov/cui. It identifies other CUI categories not specific to the Defense Index, but that may apply or relate to the Executive Branch. Since various DoD Components interact and share inter-dependencies with other departments, agencies, and activities in the Executive Branch, it is important to know and understand these indexes and categories, along with their associated markings, in order to recognize other agencies' CUI and handle the information accordingly. Of note, the CUI indexes and categories listed in the CUI Registry and DoD CUI Registry identify the safeguarding and dissemination requirements as identified by the related law, regulation, or government-wide policy. Moreover, the CUI Registry is agile and subject to change based on changes in law, regulation, or government-wide policy.

g. In accordance with ISOO Notice 2016-01, CUI training standards must, at minimum:

(1) Identify individual responsibilities for protecting CUI.

(2) Identify the organizational index with CUI categories routinely handled by DoD personnel.

(3) Describe the CUI Registry, including purpose, structure, and location (http://www.archives.gov/cui).

(4) Describe the differences between CUI Basic and CUI Specified.

(5) Identify the offices or organizations with DoD CUI Program oversight responsibilities.

(6) Address CUI marking requirements as described in this issuance.

(7) Address the required physical safeguards and CUI protection methods as described in this issuance.

(8) Address the destruction requirements and methods as described in this issuance.

(9) Address the incident reporting procedures as described in this issuance.

(10) Address methods for properly disseminating CUI within the DoD and with external entities inside and outside of the Executive Branch.

(11) Address the methods for properly decontrolling CUI as described in this issuance.

3.7. GENERAL DOD CUI REQUIREMENTS.

This section specifies initial requirements for implementing, marking, and managing the CUI program. Table 1 contains a sample list of the categories found in the DoD CUI Registry and Defense Index. A complete list of CUI Indexes and Categories can be found on Intelink at https://intelshare.intelink.gov/sites/ousdi/hcis/sec/icdirect/information/CUI/Forms/AllItems.aspx. Some significant points about DoD CUI include:

a. CUI does not include information lawfully and publicly available without restrictions.

b. CUI requires safeguarding measures identified by the CUI EA in Part 2002.14 of Title 32, CFR and, as necessary, in the law, regulation, or government-wide policy with which it is associated. DoD CUI may be disseminated to DoD personnel to conduct official DoD and U.S. Government business in accordance with a law, regulation, or government-wide policy.

(1) No individual may have access to CUI information unless it is determined he or she has an authorized, lawful government purpose.

(2) The person with authorized possession, knowledge, or control of CUI will determine whether an individual has an authorized, lawful government purpose to access designated CUI.

(3) CUI information may be disseminated within the DoD Components and between DoD Component officials and DoD contractors, consultants, and grantees to conduct official

business for the DoD, provided dissemination is consistent with controls imposed by a distribution statement or limited dissemination controls (LDC).

(4) CUI designated information may be disseminated to a foreign recipient in order to conduct official business for the DoD, provided the dissemination has been approved by a disclosure authority in accordance with Paragraph 3.4.c. and the CUI is appropriately marked as releasable to the intended foreign recipient.

c. CTI compiled or aggregated may become classified. Such classified CTI is subject to the requirements of the National Industrial Security Program, which has different requirements than Section 252.204-7012 of the DFARS for unclassified CTI.

(1) CTI is to be marked with one of the Distribution Statements B through F, in accordance with DoDI 5230.24.

(2) Pursuant to section 252.204-7012 of the DFARS, scientific, technical, and engineering information beyond basic research(known as pre-applied research and development aligning with the Science, Technology, and Engineering Information Program policies, with military or space application subject to controls on the access, use, reproduction, modification, performance, transmission, display, release, disclosure, or dissemination) shall be treated as CUI. This type of information or data can become classified by compilation or aggregation and is subject to the National Disclosure Policy (NDP-1). Examples include preliminary research and engineering data, engineering drawings, and associated specifications, lists, standards, process sheets, manuals, technical reports, technical orders, studies and analyses on topics requested by DoD Components, catalog-item identifications, data sets, and computer software with executable or source code.

d. As DoD programs transition through the acquisition life cycle, the CUI category or treatment of information may change. In accordance with Title 32, CFR, if the safeguarding requirements for a CUI category or the original law, regulation, or government-wide policy changes, there will be a cascading effect requiring changes for the particular category. These changes will be implemented as soon as possible.

(1) For example, in the acquisition area, a program will begin in the basic research and development phase. Once this program milestone is achieved, the project could transition to the applied research and development or to the production phase.

(2) At this point, the original CUI must be reviewed for any necessary adjustments, including potential changes to the CUI designation, category, subcategory or type, or controls.

e. CUI will be identified in SCGs to ensure such information receives appropriate protection. If the SCG is canceled, a memorandum or other guidance document may be issued to identify CUI instead.

f. DoD is required to provide documents and records requested by members of the public, unless those records are exempt from disclosure in accordance with the procedures established by Part 286 of Title 32, CFR and DoDD 5400.07.

g. Other CUI category information may qualify for withholding from public release based on a specific FOIA exemption for the type of information in question. Determining whether information meets the requirements for CUI shall be done separately and prior to identifying any potential FOIA exemptions.

h. CUI requiring distribution statements in accordance with DODI 5230.24 or the LDC identified in the related law, regulation, or government-wide policy, but does not qualify as classified information in accordance with E.O. 13526 or Chapter 14 of Title 42, U.S.C, (also known and referred to in this issuance as the "Atomic Energy Act of 1954"), will be implemented in accordance with this issuance.

i. Table 1 is an example of the format for the list of all DoD CUI Registry Categories aligned to the CUI National Registry published on Intelink at https://intelshare.intelink.gov/sites/ousdi/hcis/sec/icdirect/information/CUI/Forms/AllItems.aspx.

j. Table 1 provides a sample of the cross-walk of the National CUI registry to the DoD issuance(s) related to the category. The items in Table 1 identify the two unique types of data used by the Department of Energy, the DoD, and the DoD Components. Both types satisfy the CUI requirements and are subject to safeguarding and limited distribution control, and are exempt from mandatory public disclosure in accordance with Exemption 3 of the FOIA.

Table 1. DoD CUI Registry Category Examples

Category	Proposed Defense Description	Additional Information (How Used, Examples, etc.)	Authority	DoD Guidance	Miscellaneous Information
NNPI	Related to the safety of reactors and associated naval nuclear propulsion plants, and control of radiation and radioactivity associated with naval nuclear propulsion activities, including prescribing and enforcing standards and regulations for these areas as they affect the environment and the safety and health of workers, operators, and the general public. This subcategory of Defense CUI relates to the protection of information concerning nuclear reactors, materials, or security and concerns the safeguarding of nuclear reactors, materials, or security. Refer to Office of the Chief of Naval Operations Instruction N9210.3, and CG-RN-1, Revision 3, Department of Energy-DoD Classification Guide for the Naval Nuclear Propulsion Program for guidance on determining information as Unclassified Defense-NNPI.	Data and information related to the safety of reactors and associated naval nuclear propulsion plants, the control of radiation and radioactivity associated with Defense naval nuclear propulsion activities containing prescriptive and enforcement standards and regulations for these areas as they affect the environment and the safety and health of workers, operators, and the general public.	Section 2013 of Title 42, U.S.C.; Section 2511 of Title 50, U.S.C.	Chief of Naval Operations Instruction N9210.3, and CG-RN-1, Revision 3.	Sanctions: Section 2168 and 2168(b) of Title 42, U.S.C. **The DoD NNPI is unique as it is exempt from mandatory public disclosure under Exemption 3 of the FOIA.**
Unclassified Controlled Nuclear Information - Defense	Relating to Department of Defense special nuclear material (SNM), equipment, and facilities, as defined by Part 223 of Title 32, CFR. This type of Defense CUI is unclassified information about SNM security measures, DoD SNM equipment, DoD SNM facilities, or nuclear weapons in DoD custody. Information is designated DoD unclassified controlled nuclear information (UCNI) in accordance with DoDI 5210.83 only when it is determined its UD could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of the illegal production of nuclear weapons or the theft, diversion, or sabotage of DoD SNM, DoD SNM equipment, DoD SNM facilities, or nuclear weapons in DoD custody.	This type of Defense CUI may be designated UCNI by the Heads of the DoD Components and individuals delegated authority in accordance with DoDD 5210.83. Some specific examples include: Security plans, procedures, and equipment used for the physical safeguarding of DoD SNM.	Section 128(a) of Title 10, U.S.C.; Part 223 of Title 32, CFR	DoDD 5210.83; DoDI 5210.83;	**The DoD UCNI is unique as it is exempt from mandatory public disclosure under Exemption 3 of the FOIA.**

k. Restricted data or formerly restricted data are classified and shall not be commingled with CUI in an unclassified document. For restricted data or formerly restricted data, follow the marking requirements in accordance with Volume 2 of DoDM 5200.01; Part 1045 of Title 10, CFR; and the Atomic Energy Act of 1954.

l. For DoD Geospatial intelligence information and data, the DoD will not apply the Geodetic Product Information (GPI) designation. Instead, the DoD will continue to use the designation for "Limited Distribution" with the marking of "LIMDIS." For all other DoD geospatial information and data, such as installation geospatial information and services (IGI&S) as defined by DoDI 8130.01, use the GPI category or other appropriate CUI category designations defined by this issuance. The DoD will use the GPI designation for all of the non-Geospatial intelligence information and data. Approved LDCs for the DoD are located on Intelink at https://intelshare.intelink.gov/sites/ousdi/hcis/sec/icdirect/information/CUI/Forms/AllItems.aspx.

m. The request for a waiver for a particular CUI Program requirement will be handled in accordance with Volume 1 of DoDM 5200.01 for CNSI.

n. DoD Component heads shall produce annual self-inspection reports and general program status updates to fulfill ISOO monitoring and reporting requirements.

3.8. OCA.

DoD OCAs will determine if CUI under their control, when compiled, is classified. If so, the applicable SCGs must address the compilation. Any time an OCA discovers that compiled or aggregated information is not properly classified on websites, folders, or documents, the OCA will:

a. Notify the organization using the compiled information to remove or protect the information.

b. Conduct a damage assessment.

c. Determine if the information still requires classified protection in its compiled form. If not, the OCA must document the revised aggregation or compilation determination by updating SCGs and providing the guide to all users in accordance with DoDM 5200.45.

d. If the information is determined not to be classified, it must be reviewed to identify if the information is CUI.

e. Since OCAs are the owners of the information under their authority, they are authorized to identify and mark such information as CUI.

3.9. GENERAL RELEASE AND DISCLOSURE REQUIREMENTS.

a. The release or disclosure to foreign governments, international organizations, coalitions, or allied personnel of CUI not controlled as NOFORN will be in accordance with a law, regulation, or government-wide policy. Access to such CUI during official foreign national visits and assignments to DoD Components and cleared contractor facilities, when applied by contract, will be in accordance with DoDD 5230.20.

b. CUI not controlled as NOFORN may be released or disclosed to non-U.S. citizens employed by the DoD if:

(1) Access to such information is within the scope of their assigned duties.

(2) Access to such information would help accomplish a lawful and authorized DoD mission or purpose and would not be detrimental to the interests of the DoD or the U.S. Government.

(3) There are no contract restrictions prohibiting access to such information.

(4) Access to such information is in accordance with DoDIs 8500.01 and 5200.02 and export control regulations, as applicable.

c. The DoD Components' CSAOs and CPMs will establish procedures to ensure prompt and appropriate management action is taken in cases of CUI misuse, including UD of CUI, improper CUI designation and marking, violation of this issuance, and incidents potentially placing CUI at risk of UD. Such actions will focus on correcting or eliminating the conditions contributing to the incident.

d. For UD of CUI, no formal security inquiry or investigation is required unless disciplinary action will be taken against the individual(s) responsible. In such cases, a preliminary inquiry is appropriate. UD of certain CUI, such as export controlled-technical data, may also result in potential civil and criminal sanctions against responsible persons based on the procedures codified in the relevant law, regulation, or government-wide policy. The DoD Component originating the CUI will be informed of any UD.

e. Reporting or accounting for UD of CUI shall be done in accordance with Paragraph 3.5.a(4), and the appropriate Military Department Counterintelligence Organization shall be notified of all incidents.

3.10. GENERAL SYSTEM AND NETWORK CUI REQUIREMENTS.

In accordance with DoDIs 8500.01 and 8510.01, security controls for systems and networks are set to the level required by the safeguarding requirements for the data or information being processed, as identified in Federal Information Processing Standards 199 and 200. For DoD CUI, the minimum security level will be moderate confidentiality in accordance with Part 2002 of Title 32, CFR and NIST SP 800-171.

a. The USD(I&S) will notify and coordinate with the CUI EA regarding waiver requests involving CUI requirements prior to granting any such requests, including waiver requests

related to IS. The USD(I&S) must coordinate and collaborate with the DoD CIO to ensure the agency requesting the waiver has plans to appropriately safeguard and control CUI. The request for a waiver for a CUI Program requirement shall be done in accordance with Volume 1 of DoDM 5200.01 for CNSI, as modified in the forthcoming manual supporting this instruction.

b. DoD personnel will not use unofficial or personal (e.g., .net; .com) e-mail accounts, messaging systems, or other non-DoD information systems, except approved or authorized government contractor systems, to conduct official business involving CUI. This is necessary to ensure proper accountability for Federal records and to facilitate data spill remediation in accordance with Public Law 113-187 and the January 16, 2018 Deputy Secretary of Defense memorandum.

c. DoD information systems processing, storing, or transmitting CUI will be categorized at the moderate impact level, and follow the guidance in DoDIs 8500.01 and 8510.01. Non-DoD information systems processing, storing, or transmitting CUI will provide adequate security, and the appropriate requirements must be incorporated into all contacts, grants, and other legal agreements with non-DoD entities in accordance with DoDI 8582.01. The NIST SP 800-171 governs and protects CUI on non-Federal IS when applied by contract.

d. For systems, networks, and programs operating on the various domains, a splash screen warning and notice of consent, as shown in Figure 3, must be employed to alert users of CUI within the program. This ensures proper safeguarding and dissemination controls are implemented in accordance with Part 2002 of Title 32, CFR and this issuance.

Figure 3. Notice and Consent

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

e. Organizations will modify or install classification marking tools on UNCLASSIFIED, SECRET, and TOP SECRET network systems to account for CUI information and readily permit inclusion of CUI markings and designator indicators as required by Part 2002 of Title 32, CFR.

SECTION 4: DISSEMINATION, DECONTROLLING, AND DESTRUCTION OF CUI

4.1. GENERAL.

Part 2002 of Title 32, CFR requires dissemination statements to be placed on classified and unclassified documents or other materials when CUI necessitates access restrictions, including those required by law, regulation, or government-wide policy. These statements facilitate control, secondary sharing, decontrol, and release without the need to repeatedly obtain approval or authorization from the controlling DoD office.

a. Dissemination controls identify the audience deemed to have a lawful government purpose to use the CUI and specify the rationale for applying the controls by specific codes in accordance with DoDI 5230.24 and this issuance.

b. Agencies must promptly decontrol CUI properly determined by the CUI owner to no longer require safeguarding or dissemination controls, unless doing so conflicts with the related law, regulation, or government-wide policy in accordance with DoDI 5230.09.

c. Decontrolling CUI through the public release process relieves authorized holders from requirements for handling information in accordance with the CUI Program. A prepublication review must be conducted in accordance with DoDI 5230.09 before public release may be authorized.

d. In accordance with Part 2002.20 of Title 32, CFR, if the authorized holder of the CUI publicly releases the CUI in accordance with the designating agency's authorized procedures, this constitutes the decontrol of the document.

e. To ensure CUI protection, the following measures will be implemented:

(1) During working hours, steps will be taken to minimize the risk of access by unauthorized personnel, such as not reading, discussing, or leaving CUI information unattended where unauthorized personnel are present. After working hours, CUI information will be stored in unlocked containers, desks, or cabinets if the government or government-contract building provides security for continuous monitoring of access. If building security is not provided, the information will be stored in locked desks, file cabinets, bookcases, locked rooms, or similarly secured areas. The concept of a controlled environment means there is sufficient internal security measures in place to prevent or detect unauthorized access to CUI. For DoD, an open storage environment meets these requirements.

(2) CUI information and material may be transmitted via first class mail, parcel post, or, bulk shipments. When practical, CUI information may be transmitted electronically (e.g., data, website, or e-mail), via approved secure communications systems or systems utilizing other protective measures such as Public Key Infrastructure or transport layer security (e.g., https). Avoid wireless telephone transmission of CUI when other options are available. CUI transmission via facsimile machine is permitted; however, the sender is responsible for

determining whether appropriate protection will be available at the receiving location before transmission (e.g., facsimile machine attended by a person authorized to receive CUI; facsimile machine located in a controlled government environment).

4.2. DISSEMINATION REQUIREMENTS FOR DOD CUI.

a. In accordance with this issuance, CUI access should be encouraged and permitted to the extent the access or dissemination:

(1) Complies with the law, regulation, or government-wide policy identifying the information as CUI.

(2) Furthers a lawful government purpose.

(3) Is not restricted by an authorized LDC established by the CUI EA.

(4) Is not otherwise prohibited by any other law, regulation, or government-wide policy.

b. Agencies may place limits on disseminating CUI for a lawful government purpose only using the dissemination controls listed in Table 2 or methods authorized by a specific law, regulation, or government-wide policy.

c. When handling other Executive Branch CUI, DoD personnel will follow their governance criteria for when the application of dissemination controls and its markings are allowed, and by whom, while ensuring the policy is in accordance with Part 2002 of Title 32, CFR.

d. LDCs or distribution statements cannot unnecessarily restrict CUI access.

e. Since DoD Components need to retain certain agency-specific CUI within their organizations, DoD Components may use the limited dissemination controls to limit access to those on an accompanying dissemination list, as shown in Table 2. For example, raw data, information, or products must be processed and analyzed before determining if further dissemination is required or permitted. The Limited Dissemination Control List control will be used to address this need. The LDC list is found on Intelink at https://intelshare.intelink.gov/sites/ousdi/hcis/sec/icdirect/information/CUI/Forms/AllItems.aspx.

4.3. LEGACY DISTRIBUTION STATEMENTS.

a. Legacy CUI technical documents and materials requiring export control have used distribution statements in accordance with DoDI 5230.24 in order to address the shared responsibility between the DoD and its contractors to safeguard this information. This was done for legacy CUI creation, transmission, receipt, storage, distribution, decontrol, and approved disposition authorities, including destruction.

b. As of the effective date of this issuance, DoD personnel will use LDCs for new CUI documents and materials except export controlled technical information, which must be marked

with an export control warning in accordance with DoDI 5230.24, DoDD 5230.25, and Part 250 of Title 32, CFR. The wording of the distribution statements may not be modified to specify additional distribution, such as distribution to foreign governments. However, where other markings are authorized and used in accordance with associated law, regulation, or government-wide policy (e.g., North Atlantic Treaty Organization markings, REL TO), those markings may be used to further inform distribution decisions. Therefore, "REL TO" is authorized for use with foreign nationals once the information distribution is properly coordinated with the foreign disclosure office.

Table 2. Dissemination Control and Distribution Statement Markings

NEW LDC	ALIGNMENT TO CURRENT
NONE – Publicly Releasable **AFTER** Review	DISTRO A
No Foreign Dissemination (NOFORN / NF)	
Federal Employees Only (FED ONLY)	DISTRO B
Federal Employees and Contractors Only (FEDCON)	DISTRO C
No Dissemination to Contractors (NOCON)	
Dissemination List Controlled (DL ONLY)	DISTRO F
Authorized for Release to Certain Foreign Nationals Only (REL TO USA, LIST)	
Display Only (DISPLAY ONLY)	
Dissemination List – (Include Separate List for Government Only)*	DISTRO E
Dissemination List – (Include Separate List for Government and Contractors Only)*	DISTRO D
NONE	DISTRO X: U.S. Government Agencies and private individuals or enterprises eligible to obtain export controlled technical data in accordance with DoDD 5230.25. DISTRO X was cancelled and superseded by DISTRO C.
*The dissemination list limits access to the specified individuals, groups, or agencies and must accompany the document	

c. CUI export controlled technical information or other scientific, technical, and engineering information will still use distribution statements. Export controlled information must also be marked with an export control warning as directed in DoDI 5230.24, DoDD 5230.25, and Part 250 of Title 32, CFR.

4.4. DECONTROLLING.

Guidance for decontrolling CUI records, documents, and materials is provided in this issuance, or the CUI Registry for information categories not directly related to DoD CUI.

a. CUI documents and materials will be formally reviewed in accordance with DoDI 5230.09 before being decontrolled or released to the public.

b. The originator or other competent authority (e.g., initial FOIA denial and appellate authorities) will terminate the CUI status of specific information when the information no longer requires protection from public disclosure. When the CUI status of information is terminated in this manner, all known holders will be notified by email or other means. Upon notification, holders will remove the CUI markings. Holders will not need to retrieve records on file solely for this purpose. Information with a terminated CUI status will not be publicly released without review and approval in accordance with DoDIs 5230.09, 5230.29, and 5400.04.

4.5. DESTRUCTION.

Guidance for destroying CUI documents and materials is provided in this issuance, the CUI Registry, and ISOO Notice 2019-03. CUI documents and materials will be formally reviewed in accordance with Paragraphs 4.5.a. and 4.5.b. before approved disposition authorities are applied, including destruction. Media containing CUI must include decontrolling indicators.

a. Record and non-record copies of CUI documents will be disposed of in accordance with Chapter 33 of Title 44, U.S.C. and the DoD Components' records management directives. When destroying CUI, including in electronic form, agencies must do so in a manner making it unreadable, indecipherable, and irrecoverable. If the law, regulation, or government-wide policy specifies a method of destruction, agencies must use the method prescribed.

b. Record and non-record CUI documents may be destroyed by means approved for destroying classified information or by any other means making it unreadable, indecipherable, and unrecoverable the original information such as those identified in NIST SP 800-88 and in accordance with Section 2002.14 of Title 32, CFR.

SECTION 5: APPLICATION OF DOD INDUSTRY

5.1. GENERAL.

There is a shared responsibility between the DoD and industry, when established by contract, grants, or other legal agreements or arrangements, in the identification, creation, sharing, marking, safeguarding, storage, dissemination, decontrol, disposition, destruction, and records management of CUI documents and materials. It is essential to identify and apply the general dissemination principles and guidance as prescribed by the CUI EA in accordance with Part 2002 of Title 32, CFR. Contracts containing CUI shared from DoD or generated, managed, or transmitted by the contractor via their information systems, will be in accordance with this issuance, which will be incorporated into each DoD contract.

a. The NIST SP 800-171 identifies the baseline CUI system security requirements for industry established by Part 2002 of Title 32, CFR. Additionally, Section 252.204-7012 of the DFARS specifies a waiver process for defense contractors in accordance with NIST SP 800-171 for contractor IT or networks.

b. CUI with the potential to impact national security (e.g., information related to critical programs and technology information) may require enhanced protection. These enhanced measures would address both physical and logical procedures. Enhanced protection methods for systems hosting CUI include:

(1) Access control (e.g., restricting both physical and logical access to the systems).

(2) Audit and accountability (e.g., review and monitor system usage).

(3) Configuration management (e.g., restrict system connection to only approved resources).

(4) Identification and authentication (e.g., control issuance of end-user certificates).

(5) Incident response (e.g., ensure corrective measures are implemented in a timely manner and validate effectiveness).

(6) System and communication protection (e.g., application of encryption for data at rest and restriction of connections to uncertified, unsecured, non-organizational systems). DoD Components may implement stricter CUI encryption requirements based on a law, regulation, or government-wide policy (DHA PI 8140, requires workforce encrypt emailed PHI).

(7) System and information integrity (e.g., provide network detection tools throughout the system to identify attempted intrusions).

c. Non-DoD IS processing, storing, or transmitting CUI will be safeguarded in accordance with contractual requirements identified for the particular CUI contained in the contract, DoDI 8582.01 and Section 252.204-7012 of the DFARS or their subsequent revisions.

d. When established by contract, contractors, sub-contractors, and consultants must comply with safeguarding requirements identified in the contract for all types of CUI.

e. The program office or requiring activity must identify DoD CUI at the time of contract award and, if necessary, provide guidance on information aggregation or compilation. The program office or requiring activity must review recurring or renewed contracts for CUI to comply with this issuance.

5.2. MISUSE OR UD OF CUI.

Safeguarding requirements and incident response measures for misuse or UD of CUI must be implemented across the DoD. Senior leaders, contracting officers, commanders, and supervisors at all levels must consider and take appropriate administrative, legal, or other corrective or disciplinary action to address CUI misuse or UD commensurate with the appropriate law, regulation, or government-wide policy.

5.3. REQUIREMENTS FOR DOD CONTRACTORS.

This paragraph highlights requirements for DoD contractors.

a. Whenever DoD provides information to contractors, it must identify whether any of the information is CUI via the contracting vehicle, in whole or part, and mark such documents, material, or media in accordance with this issuance.

b. Whenever the DoD provides CUI to, or CUI is generated by, non-DoD entities, protective measures and dissemination controls, including those directed by relevant law, regulation, or government-wide policy, will be articulated in the contract, grant, or other legal agreement, as appropriate.

c. DoD contracts must require contractors to monitor CUI for aggregation and compilation based on the potential to generate classified information pursuant to security classification guidance addressing the accumulation of unclassified data or information. DoD contracts shall require contractors to report the potential classification of aggregated or compiled CUI to a DoD representative.

d. DoD personnel and contractors, pursuant to mandatory DoD contract provisions, will submit unclassified DoD information for review and approval for release in accordance with the standard DoD Component processes and DoDI 5230.09.

e. All CUI records must follow the approved mandatory disposition authorities whenever the DoD provides CUI to, or CUI is generated by, non-DoD entities in accordance with Section 1220-1236 of Title 36, CFR, Section 3301a of Title 44, U.S.C., and this issuance.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
CFR	Code of Federal Regulations
CMO	Chief Management Officer of the Department of Defense
CNSI	classified national security information
CPM	Component program manager
CSAO	Component senior agency official
CTI	controlled technical information
CUI	controlled unclassified information
DDI(CL&S)	Director For Defense Intelligence (Counterintelligence, Law Enforcement, And Security)
DCSA	Defense Counterintelligence and Security Agency
DFARS	Defense Federal Acquisition Regulation Supplement
DNI	Director of National Intelligence
DoD CIO	Department of Defense Chief Information Officer
DoDD	DoD directive
DoDI	DoD instruction
DoDM	DoD manual
EA	Executive Agent
E.O.	Executive order
FOIA	Freedom of Information Act
GPI	Geodetic Product Information
ISOO	Information Security Oversight Office
IS	information systems
LDC	limited dissemination controls
NARA	National Archives and Records Administration
NISP	National Industrial Security Program
NIST SP	National Institute of Standards and Technology Special Publication
NNPI	Naval Nuclear Propulsion Information
NOFORN or NF	not releasable to foreign nationals
OCA	original classification authority
OIG DoD	Office of the Inspector General of the Department of Defense
PFPA	Pentagon Force Protection Agency

ACRONYM	MEANING
REL TO	releasable to
SCG	security classification guide
SNM	special nuclear material
U	Unclassified information
UCNI	unclassified controlled nuclear information
UD	unauthorized disclosure
U.S.C.	United States Code
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USD(R&E)	Under Secretary of Defense for Research and Engineering

G.2. DEFINITIONS.

Unless otherwise noted, these terms and their definitions are for the purpose of this issuance. Referenced definitions related to CUI in Section 2002.4 of Title 32, CFR can be found at https://intelshare.intelink.gov/sites/ousdi/hcis/sec/icdirect/information/CUI/Forms/AllItems.aspx.

TERM	DEFINITION
access	The ability or opportunity to acquire, examine, or retrieve CUI.
agency	Defined in Section 2002.4 of 32 CFR
aggregation	The creation of classified information from the accumulation of unclassified data or information from several areas within a document.
agreements and arrangements	Defined in Section 2002.4 of Title 32 CFR
authorized CUI holder	Defined in Section 2002.4 of Title 32 CFR
classified information	Defined in Section 2002.4 of Title 32 CFR
compilation	The creation of classified information resulting from the accumulation of unclassified data or information from several documents.

TERM	DEFINITION
contract	Defined in Section 252.204- 2008 and 7012 of the FARS/DFARS.
controlled environment	Defined in Section 2002.4 of Title 32 CFR
controls	Defined in Section 2002.4 of Title 32 CFR
CNSI	Defined in E.O. 13526.
CPM	Defined in Section 2002.4 of Title 32 CFR
CSAO	An official designated, in writing, by a DoD Component head who is responsible to the agency head for implementing the CUI Program. Also known as CUI SAO as defined in Section 2002.4 of Title 32 CFR
CTI	Defined in the DFARS 204.7301.
CUI	Defined in Section 2002.4 of Title 32 CFR
CUI Basic	Defined in Section 2002.4 of Title 32 CFR (DoD is not using this structure in its initial implementation phase.)
CUI category	Defined in Section 2002.4 of Title 32 CFR
CUI EA	Defined in Section 2002.4 of Title 32 CFR
CUI Indexes	An organizational grouping of CUI categories as defined by the CUI EA. The term was created by the CUI EA to replace the notion of a sub-category which implies a hierarchy structure or importance.
CUI misuse	Use of CUI in a manner not in accordance with the policy contained in E.O. 13556; Part 2002 of Title 32, CFR; the CUI Registry; agency CUI policy; or the applicable LRGWP governing the information.
CUI Program	Defined in Section 2002.4 of Title 32 CFR
CUI Registry	Defined in Section 2002.4 of Title 32 CFR
CUI Specified	Defined in Section 2002.4 of Title 32 CFR (DoD is not using this structure in its initial implementation phase.)
decontrol	Defined in Section 2002.18 of Title 32, CFR.

TERM	DEFINITION
Defense Industrial Base	Defined in the DoD Dictionary of Military and Associated Terms.
disseminating	Defined in Section 2002.4 of Title 32 CFR
document	Defined in Section 2002.4 of Title 32 CFR
DoD personnel	Defined in DoDI 5230.09.
foreign entity	Defined in Section 2002.4 of Title 32 CFR
formerly restricted data	Defined in Section 1045 of Title 10, CFR.
handling	Defined in Section 2002.4 of Title 32 CFR
lawful government purpose	Defined in Section 2002.4 of Title 32 CFR
LDC	Defined in Section 2002.4 of Title 32 CFR
legacy material	Defined in Section 2002.4 of Title 32 CFR
Limited Distribution	A legacy CUI category used by the National Geospatial-Intelligence Agency to identify a select group of sensitive, unclassified imagery or geospatial information and data created or distributed by National Geospatial Intelligence Agency or information, data, and products derived from such information (marked as LIMDIS and now referred to a GPI by CUI EA).
logical access	Electronic access controls authenticated through outside certificates accepted by the DoD to limit access to data files and systems only by vetted individuals.
misuse	Defined in Section 2002.4 of Title 32 CFR
NNPI	Information concerning the design, arrangement, development, testing, operation, administration, training, maintenance, and repair of the propulsion plants of naval nuclear powered ships and prototypes, including the associated nuclear support facilities.
non-Executive Branch entity	Defined in Section 2002.4 of Title 32 CFR

TERM	DEFINITION
personally identifiable information	Defined in Office of Management and Budget Circular No. A-130.
physical access	All DoD and non-DoD personnel entering or exiting DoD facilities or installations that authenticated a physical access control system (PACS).
portion	Defined in Section 2002.4 of Title 32 CFR
protection	Defined in Section 2002.4 of Title 32 CFR
public release	Defined in Section 2002.4 of Title 32 CFR
records	Defined in Section 2002.4 of Title 32 CFR
restricted data	Defined in Part 1045 of Title 10, CFR.
re-use	Defined in Section 2002.4 of Title 32 CFR
safeguarding	Prescribed measures and controls that protect classified information and CUI.
Senior Agency Official	An official appointed by the Secretary of Defense to be responsible for direction, administration, and oversight of the DoD's Information Security Program, including classification, declassification, CUI, safeguarding, and security education and training programs, and for the efficient and effective implementation of the guidance in this issuance.
SCG	Security classification guidance issued by an OCA identifying the elements of information regarding a specific subject requiring classification, and establishes the level and duration of classification for each element.
self-inspection	Defined in Section 2002.4 of Title 32 CFR
UD	Defined in Section 2002.4 of Title 32 CFR
unclassified	Information not requiring control, but requiring review before public release.

REFERENCES

Code of Federal Regulations, Title 10, Part 1045

Code of Federal Regulations, Title 32

Code of Federal Regulations, Title 36

Defense Federal Acquisition Regulation Supplement, Subparts 252.204-2008 and 7012, current edition

Deputy Secretary of Defense Memorandum, "Designation of Senior Agency Official for Controlled Unclassified Information," December 22, 2010

Deputy Secretary of Defense Memorandum, "Unauthorized Disclosures of Classified Information or Controlled Unclassified Information on DoD Information Systems," August 14, 2014

DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I))," October 24, 2014, as amended

DoD Directive 5200.43, "Management of the Defense Security Enterprise," October 01, 2012, as amended

DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations (NDP-1)," June 16, 1992

DoD Directive 5230.20, "Visits and Assignments of Foreign Nationals," June 22, 2005

DoD Directive 5400.07, "DoD Freedom of Information Act (FOIA) Program," April 5, 2019

DoD Instruction 2040.02, "International Transfers of Technology, Articles, and Services," March 27, 2014, as amended

DoD Instruction 3200.12, "DoD Scientific and Technical Information Program (STIP)," August 22, 2013, as amended

DoD Instruction 5015.02, "DoD Records Management Program," February 24, 2015, as amended

DoD Instruction 5200.02, "DoD Personnel Security Program (PSP), Change 2," March 21, 2014, as amended

DoD Instruction 5210.83, "DoD Unclassified Controlled Nuclear Information (UCNI)," July 12, 2012, as amended

DoD Instruction 5230.09, "Clearance of DoD Information for Public Release," January 25, 2019

DoD Instruction 5230.24, "Distribution Statements on Technical Documents," August 23, 2012, as amended

DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public Release," August 13, 2014, as amended

DoD Instruction 5400.04, "Provision of Information to Congress," March 17, 2009

DoD Instruction 5400.11, "DoD Privacy and Civil Liberties Programs," January 29, 2019

DoD Instruction 8320.07, "Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense," August 03, 2015, as amended

DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, as amended

DoD Instruction 8510.01, “Risk Management Framework (RMF) for DoD Information Technology (IT),” March 12, 2014, as amended

DoD Manual 5200.01, Volume 1, “DoD Information Security Program: Overview, Classification, And Declassification,” February 24, 2012, as amended

DoD Manual 5200.01, Volume 2, “DoD Information Security Program: Marking of Information,” February 24, 2012, as amended

DoD Manual 5200.45, “Instruction for Developing Security Classification Guides,” April 02, 2013, as amended

DoD Manual 5400.07, “DoD Freedom of Information Act (FOIA) Program,” January 25, 2017

Executive Order 13526, “Classified National Security Information,” December 29, 2009

Executive Order 13556, “Controlled Unclassified Information,” November 04, 2010

Federal Information Processing Standards Publication 199, “Standards for Security Categorization of Federal Information and Information Systems,” February 2004

Federal Information Processing Standards Publication 200, “Minimum Security Requirements for Federal Information and Information Systems,” March 2006

Information Security Oversight Office, “CUI Notice 2016-01: Implementation Guidance for the Controlled Unclassified Information Program,” September 14, 2016

Information Security Oversight Office, “CUI Notice: Decontrolling Controlled Unclassified

Information (CUI) in Response to a Freedom of Information Act (FOIA) Request,”

November 19, 2018

Information Security Oversight Office, “CUI Notice 2019-01: Controlled Unclassified Information (CUI) Coversheets and Labels,” February 22, 2019

Information Security Oversight Office, “CUI Notice 2019-02: CUI Program Manage Position Description Template,” May 13, 2019

Information Security Oversight Office, “CUI Notice 2019-03: Destroying Controlled Unclassified Information (CUI),” July 15, 2019

Information Security Oversight Office Response Letter to Under Secretary of Defense for Intelligence and Security, August 21, 2019

Information Security Oversight Office Response Letter to Under Secretary of Defense for Intelligence, Subject: “Unclassified versus Uncontrolled Unclassified Information”, June 4, 2019

Intelligence Community Directive 710, “Classification Management and Control Markings System,” June 21, 2013

Intelligence Community Policy Guidance 403.1, “Criteria for Foreign Disclosure and release of Classified National Intelligence,” June 21, 2013

National Institute of Standards and Technology Special Publication 800-171, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations,” January 14, 2016, as amended

National Institute of Standards and Technology Special Publication 800-88, Revision 1, “Guidelines for Media Sanitization,” February 5, 2015

National Strategy for Information Sharing and Safeguarding, December 19, 2012

Office of the Chairman of the Joint Chiefs of Staff, “DoD Dictionary of Military and Associated Terms,” current edition

Office of the Chief of Naval Operations Instruction N9210.3, “Safeguarding of Naval Nuclear Propulsion Information (NNPI),” June 7, 2010

Office of Management and Budget Circular No. A-130, “Managing Information as a Strategic Resource,” July 28, 2016

OPNAVINST N9210.3, “Safeguarding of Naval Nuclear Propulsion Information (NNPI)”, June 07, 2010

Under Secretary of Defense for Intelligence Memorandum, “Controlled Unclassified Information Implementation and Oversight for the Defense Industrial Base,” May 17, 2018

United States Code, Title 5

United States Code, Title 10

United States Code, Title 42, Chapter 14 (also known as the “Atomic Energy Act of 1954”)

United States Code, Title 44

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide

U.S. Department of Commerce
Gina M. Raimondo, Secretary
National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

NIST Special Publication
NIST SP 1300
https://doi.org/10.6028/NIST.SP.1300
February 2024

NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide Overview

Purpose

This guide provides small-to-medium sized businesses (SMB), specifically those who have modest or no cybersecurity plans in place, with considerations to kick-start their cybersecurity risk management strategy by using the NIST Cybersecurity Framework (CSF) 2.0. The guide also can assist other relatively small organizations, such as non-profits, government agencies, and schools. It is a supplement to the NIST CSF and is not intended to replace it.

What is the NIST Cybersecurity Framework?

The NIST Cybersecurity Framework is voluntary guidance that helps organizations —regardless of size, sector, or maturity— better **understand**, **assess**, **prioritize**, and **communicate** their cybersecurity efforts. The Framework is not a one-size-fits-all approach to managing cybersecurity risks. This supplement and the full CSF 2.0 can help organizations to consider and record their own risk tolerances, priorities, threats, vulnerabilities, requirements, etc.

Getting Started with the Cybersecurity Framework

The CSF organizes cybersecurity outcomes into six high-level Functions: Govern, Identify, Protect, Detect, Respond, and Recover. These Functions, when considered together, provide a comprehensive view of managing cybersecurity risk. The activities listed for each Function within this guide may offer a good starting point for your business. For specific, action-oriented examples of how to achieve the listed activities, reference the CSF 2.0 Implementation Examples. If there are activities contained within this guide that you do not understand or do not feel comfortable addressing yourself, this guide can serve as a discussion prompt with whomever you have chosen to help you reduce your cybersecurity risks, such as a managed security service provider (MSSP).

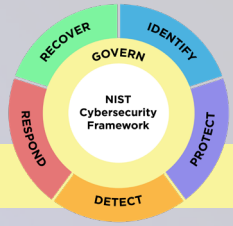
EXPLORE MORE CSF 2.0 RESOURCES

nist.gov/cyberframework

Quickly find what you need, including:

- ✓A suite of NEW Quick Start Guides
- ✓Implementation Examples
- ✓Search tools
- ✓FAQs
- ✓And much more!

GOVERN



The Govern Function helps you establish and monitor your business's cybersecurity risk management strategy, expectations, and policy.

Actions to Consider

Understand

- Understand how cybersecurity risks can disrupt achievement of your business's mission. *(GV.OC-01)*
- Understand your legal, regulatory, and contractual cybersecurity requirements. *(GV.OC-03)*
- Understand who within your business will be responsible for developing and executing the cybersecurity strategy. *(GV.RR-02)*

Assess

- Assess the potential impact of a total or partial loss of critical business assets and operations. *(GV.0C-04)*
- Assess whether cybersecurity insurance is appropriate for your business. *(GV.RM-04)*
- Assess cybersecurity risks posed by suppliers and other third parties before entering into formal relationships. *(GV.SC-06)*

Prioritize

- Prioritize managing cybersecurity risks alongside other business risks. *(GV.RM-03)*

Communicate

- Communicate leadership's support of a risk-aware, ethical, and continually improving culture. *(GV.RR-01)*
- Communicate, enforce, and maintain policies for managing cybersecurity risks. *(GV.PO-01)*

Getting Started with Cybersecurity Governance

You can use these tables to begin thinking about your cybersecurity governance strategy.

Setting Organizational Context	
Our business mission statement:	
What cybersecurity risks may prevent us from achieving this mission?	

Documenting Cybersecurity Requirements	
List your legal requirements:	
List your regulatory requirements:	
List your contractual requirements:	

Technical Deep Dive: Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight

Questions to Consider

- As our business grows, how often are we reviewing our cybersecurity strategy?
- Do we need to upskill our existing staff, hire talent, or engage an external partner to help us establish and manage our cybersecurity plan?
- Do we have acceptable use policies in place for business and for employee-owned devices accessing business resources? Have employees been educated on these policies?

Related Resources

- Securing Small and Medium-Sized Supply Chains Resource Handbook
- Choosing A Vendor/Service Provider

View all NIST CSF 2.0 Resources Here

IDENTIFY

The Identify Function helps you determine the current cybersecurity risk to the business.

Actions to Consider

Understand

- Understand what assets your business relies upon by creating and maintaining an inventory of hardware, software, systems, and services. *(ID.AM-01/02/04)*

Assess

- Assess your assets (IT and physical) for potential vulnerabilities. *(ID.RA-01)*
- Assess the effectiveness of the business's cybersecurity program to identify areas that need improvement. *(ID.IM-01)*

Prioritize

- Prioritize inventorying and classifying your business data. *(ID.AM-07)*
- Prioritize documenting internal and external cybersecurity threats and associated responses using a risk register. *(ID.RA)*

Communicate

- Communicate cybersecurity plans, policies, and best practices to all staff and relevant third parties. *(ID.IM-04)*
- Communicate to staff the importance of identifying needed improvements to cybersecurity risk management processes, procedures, and activities. *(ID.IM)*

Getting Started with Identifying Current Cybersecurity Risk to Your Business

Before you can protect your assets, you need to identify them. Then you can determine the appropriate level of protection for each asset based upon its sensitivity and criticality to your business mission. You can use this sample table to get started on your information technology (IT) asset inventory. As your business matures, you might consider using an automated asset inventory solution or a managed security service provider to help you manage all your business assets.

Software/ hardware/ system/ service	Asset's official use:	Asset administrator or owner:	Identify sensitive data the asset has access to:	Is multi-factor authentication required to access this asset?	Risk to business if we lose access to this asset

Technical Deep Dive: Integrating Cybersecurity and Enterprise Risk Management

Questions to Consider

- What are our most critical business assets (data, hardware, software, systems, facilities, services, people, etc.) we need to protect?
- What are the cybersecurity and privacy risks associated with each asset?
- What technologies or services are personnel using to accomplish their work? Are these services or technologies secure and approved for use?

Related Resources

- NIST Risk Register Template
- Take Stock. Know What Sensitive Information You Have
- Evaluating Your Operational Resilience and Cybersecurity Practices

View all NIST CSF 2.0 Resources Here

PROTECT

The Protect Function supports your ability to use safeguards to prevent or reduce cybersecurity risks.

Actions to Consider

Understand

- Understand what information employees should or do have access to. Restrict sensitive information access to only those employees who need it to do their jobs. *(PR.AA-05)*

Assess

- Assess the timeliness, quality, and frequency of your company's cybersecurity training for employees. *(PR.AT-01/02)*

Prioritize

- Prioritize requiring multi-factor authentication on all accounts that offer it and consider using password managers to help you and your staff generate and protect strong passwords. *(PR.AA-03)*
- Prioritize changing default manufacturer passwords. *(PR.AA-01)*
- Prioritize regularly updating and patching software and operating systems. Enable automatic updates to help you remember. *(PR.PS-02)*
- Prioritize regularly backing up your data and testing your backups. *(PR.DS-11)*
- Prioritize configuring your tablets and laptops to enable full-disk encryption to protect data. *(PR.DS-01)*

Communicate

- Communicate to your staff how to recognize common attacks, report attacks or suspicious activity, and perform basic cyber hygiene tasks. *(PR.AT-01/02)*

Getting Started with Protecting Your Business

Enabling multi-factor authentication (MFA) is one of the fastest, cheapest ways you can protect your data. Start with accounts that can access the most sensitive information. Use this checklist to give you a head start, but remember your own list will be longer than this:

Account	MFA Enabled (Y/N)
Banking Account(s)	
Accounting and Tax Account(s)	
Merchant Account(s)	
Google, Microsoft, and/or Apple ID Account(s)	
Email Account(s)	
Password Manager(s)	
Website Account(s)	

Technical Deep Dive: NIST Digital Identity Guidelines

Questions to Consider

- Are we restricting access and privileges only to those who need it? Are we removing access when they no longer need it?
- How are we securely sanitizing and destroying data and data storage devices when they're no longer needed?
- Do employees possess the knowledge and skills to perform their jobs with security in mind?

Related Resources

- Cybersecurity Training Resources
- Multi-Factor Authentication
- Protecting Your Business from Phishing

View all NIST CSF 2.0 Resources Here

DETECT

The Detect Function provides outcomes that help you find and analyze possible cybersecurity attacks and compromises.

Actions to Consider

Understand

- Understand how to identify common indicators of a cybersecurity incident. *(DE.CM)*

Assess

- Assess your computing technologies and external services for deviations from expected or typical behavior. *(DE.CM-06/09)*
- Assess your physical environment for signs of tampering or suspicious activity. *(DE.CM-02)*

Prioritize

- Prioritize installing and maintaining antivirus and anti-malware software on all business devices—including servers, desktops and laptops. *(DE.CM-09)*
- Prioritize engaging a service provider to monitor computers and networks for suspicious activity if you don't have the resources to do it internally. *(DE.CM)*

Communicate

- Communicate with your authorized incident responder, such as an MSSP, about the relevant details from the incident to help them analyze and mitigate it. *(DE.AE-06/07)*

Getting Started with Detecting Incidents

Some common indicators of a cybersecurity incident are:

- Loss of usual access to data, applications, or services
- Unusually sluggish network
- Antivirus software alerts when it detects that a host is infected with malware
- Multiple failed login attempts
- An email administrator sees many bounced emails with suspicious content
- A network administrator notices an unusual deviation from typical network traffic flows

Technical Deep Dive: NIST Computer Security Incident Handling Guide

Questions to Consider

- Do devices that are used for our business, whether business-owned or employee-owned, have antivirus software installed?
- Do employees know how to detect possible cybersecurity attacks and how to report them?
- How is our business monitoring its logs and alerts to detect potential cyber incidents?

Related Resources

- Ransomware Protection and Response
- Detecting a Potential Intrusion
- Cybersecurity Training Resources

View all NIST CSF 2.0 Resources Here

RESPOND

The Respond Function supports your ability to take action regarding a detected cybersecurity incident.

Actions to Consider

Understand

- Understand what your incident response plan is and who has authority and responsibility for implementing various aspects of the plan. *(RS.MA-01)*

Assess

- Assess your ability to respond to a cybersecurity incident. *(RS.MA-01)*
- Assess the incident to determine its severity, what happened, and its root cause. *(RS.AN-03, RS.MA-03)*

Prioritize

- Prioritize taking steps to contain and eradicate the incident to prevent further damage. *(RS.MI)*

Communicate

- Communicate a confirmed cybersecurity incident with all internal and external stakeholders (e.g., customers, business partners, law enforcement agencies, regulatory bodies) as required by laws, regulations, contracts, or policies. *(RS.CO-02/03)*

Getting Started with an Incident Response Plan

Before an incident occurs, you want to be ready with a basic response plan. This will be customized based on the business but should include:

- ✓ **A business champion**: Someone who is responsible for developing and maintaining your incident response plan.
- ✓ **Who to call:** List all the individuals who may be part of your incident response efforts. Include their contact information, responsibilities, and authority.
- ✓ **What/when/how to report:** List your business's communications/reporting responsibilities as required by laws, regulations, contracts, or policies.

Technical Deep Dive: NIST Computer Security Incident Handling Guide

Contact	Phone
Business Leader:	
Technical Contact:	
State Police:	
Legal:	
Bank:	
Insurance:	

Questions to Consider

- Do we have a cybersecurity incident response plan? If so, have we practiced it to see if it is feasible?
- Do we know who the key internal and external stakeholders and decision-makers are who will assist if we have a confirmed cybersecurity incident?

Related Resources

- Incident Response Plan Basics
- FBI's Internet Crime Complaint Center
- Data Breach Response: A Guide for Business
- Best Practices for Victim Response and Reporting of Cyber Incidents

View all NIST CSF 2.0 Resources Here

RECOVER

The Recover Function involves activities to restore assets and operations that were impacted by a cybersecurity incident.

Actions to Consider

Understand

- Understand who within and outside your business has recovery responsibilities. *(RC.RP-01)*

Assess

- Assess what happened by preparing an after-action report—on your own or in consultation with a vendor/partner—that documents the incident, the response and recovery actions taken, and lessons learned. *(RC.RP-06)*
- Assess the integrity of your backed-up data and assets before using them for restoration. *(RC.RP-03)*

Prioritize

- Prioritize your recovery actions based on organizational needs, resources, and assets impacted. *(RC.RP-02)*

Communicate

- Communicate regularly and securely with internal and external stakeholders. *(RC.CO)*
- Communicate and document completion of the incident and resumption of normal activities. *(RC.RP-06)*

Getting Started with a Recovery Playbook

A playbook typically includes the following critical elements:

- ✓ A set of formal recovery processes
- ✓ Documentation of the criticality of organizational resources (e.g., people, facilities, technical components, external services)
- ✓ Documentation of systems that process and store organizational information, particularly key assets. This will help inform the order of restoration priority
- ✓ A list of personnel who will be responsible for defining and implementing recovery plans
- ✓ A comprehensive recovery communications plan

Technical Deep Dive: NIST Guide for Cybersecurity Event Recovery

Questions to Consider

- What are our lessons learned? How can we minimize the chances of a cybersecurity incident happening in the future?
- What are our legal, regulatory, and contractual obligations for communicating to internal and external stakeholders about a cybersecurity incident?
- How do we ensure that the recovery steps we are taking are not introducing new vulnerabilities to our business?

Related Resources

- Cybersecurity Training Resources
- Creating an IT Disaster Recovery Plan
- Backup and Recover Resources

View all NIST CSF 2.0 Resources Here

Profiles and Additional Resources

Using Organizational Profiles to Implement the Cybersecurity Framework

A *CSF Organizational Profile* describes an organization's current and/or target cybersecurity posture in terms of the CSF Core's cybersecurity outcomes. Every Organizational Profile includes one or both of the following:

1. A **Current Profile** specifies the desired outcomes an organization is currently achieving (or attempting to achieve) and characterizes how or to what extent each outcome is being achieved.
2. A **Target Profile** specifies the outcomes an organization has selected and prioritized for achieving its cybersecurity risk management objectives.
   - You can also use a **Community Profile** as the basis for your Target Profile. A Community Profile is a baseline of targeted outcomes for a particular sector, technology, threat type, or other use case.
   - You can also choose to use the **CSF Tiers** to inform your Profile creation. Tiers characterize the current or targeted rigor of an organization's practices by CSF Function or Category. See the *Quick-Start Guide for Using the CSF Tiers* for more information on Tiers and their use.

View the *Quick-Start Guide for Creating and Using Organizational Profiles* for more detailed information on how to get started creating Current and Target Profiles for your organization.

Additional Resources

The NIST Cybersecurity Framework Reference Tool allows users to explore the full CSF 2.0 Core in human and machine-readable versions (in JSON and Excel), while also maintaining resources with information to help you achieve your desired outcomes, such as:

- Mapping: Informative references are mappings indicating relationships between the CSF 2.0 and various standards, guidelines, regulations, and other content. They help inform how an organization may achieve the Core's outcomes.
- Implementation examples provide illustrations of concise, action-oriented steps to guide organizations in achieving the CSF outcomes. The examples are not a comprehensive list of all actions that could be taken by an organization, nor are they a baseline of required actions; they are a set of helpful examples to get organizations thinking about concrete steps.

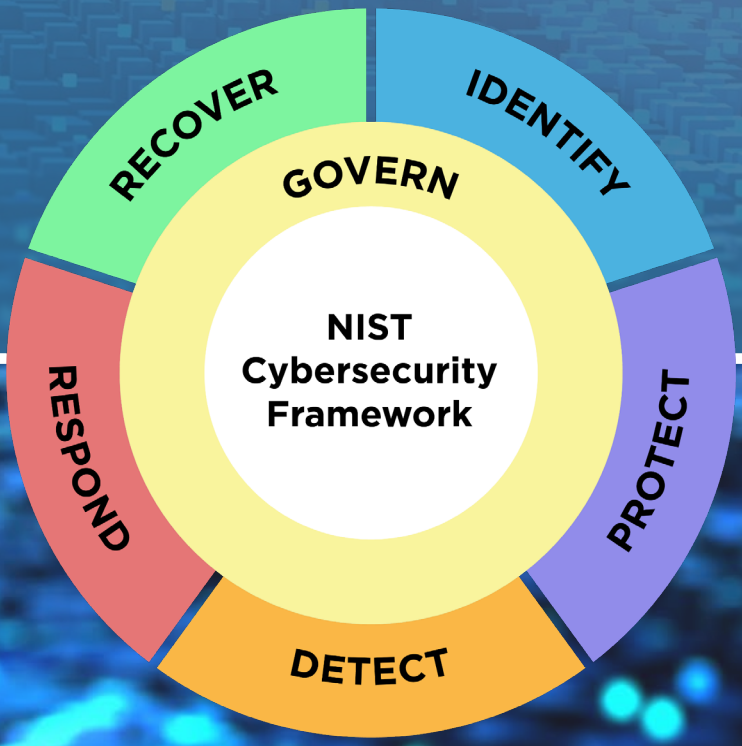
NIST Cybersecurity and Privacy Reference Tool (CPRT) provides a simple way to access reference data from various NIST cybersecurity and privacy standards, guidelines, and Frameworks–downloadable in common formats (XLSX and JSON).

NIST SP 800-53 provides a catalog of security and privacy controls you can choose from. The controls are flexible, customizable, and implemented as part of an organization-wide process to manage risk. View and export from the Cybersecurity and Privacy Reference Tool (CPRT).

The Workforce Framework for Cybersecurity (NICE Framework) helps employers achieve the outcomes in the CSF 2.0 by assisting them to identify critical gaps in cybersecurity staffing and capabilities; determine and communicate position responsibilities and job descriptions; and provide staff training and career pathways.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Cybersecurity Framework 2.0: RESOURCE & OVERVIEW GUIDE



NIST Special Publication
NIST SP 1299

https://doi.org/10.6028/NIST.SP.1299
February 2024

NIST CSF 2.0:
RESOURCE & OVERVIEW GUIDE

WHAT IS THE CSF 2.0…AND POPULAR WAYS TO USE IT?

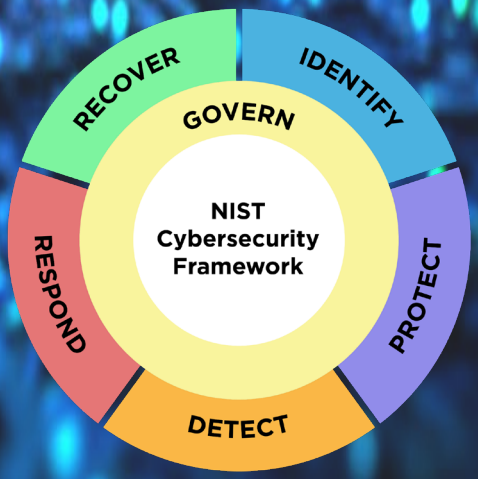
The NIST Cybersecurity Framework (CSF) 2.0 can help organizations manage and reduce their cybersecurity risks as they start or improve their cybersecurity program. The CSF outlines specific outcomes that organizations can achieve to address risk. Other NIST resources help explain specific actions that can be taken to achieve each outcome. *This guide is a supplement to the NIST CSF and is not intended to replace it.*

The CSF 2.0, along with NIST's supplementary resources, can be used by organizations to understand, assess, prioritize, and communicate cybersecurity risks; it is particularly useful for fostering internal and external communication across teams — as well as integrating with broader risk management strategies.

The CSF 2.0 is organized by six Functions — **Govern, Identify, Protect, Detect, Respond,** and **Recover.** Together, these Functions provide a comprehensive view for managing cybersecurity risk. This *Resource & Overview Guide* offers details about each Function to serve as potential starting points.

The CSF 2.0 is comprised of:

- **CSF Core** - A taxonomy of high-level cybersecurity outcomes that can help any organization manage its cybersecurity risks.
- **CSF Organizational Profiles** - A mechanism for describing an organization's current and/or target cybersecurity posture in terms of the CSF Core's outcomes.
- **CSF Tiers** - Can be applied to CSF Organizational Profiles to characterize the rigor of an organization's cybersecurity risk governance and management practices.



NIST CSF 2.0:
RESOURCE & OVERVIEW GUIDE

EXPLORE MORE CSF 2.0 RESOURCES

Informative References	**View and create mappings between CSF 2.0 and other documents.** Do you want to submit your mappings to NIST documents and have them displayed on our site? Please follow the link to the left or email olir@nist.gov if you have any questions.
Cybersecurity & Privacy Reference Tool (CPRT)	**Browse and download the CSF 2.0 Core & mapped content**. CPRT provides a centralized, standardized, and modernized mechanism for managing reference datasets (and offers a consistent format for accessing reference data from various NIST cybersecurity and privacy standards, guidelines, and frameworks).
Implementation Examples	View and download notional examples of concise, action-oriented steps to help achieve the outcomes of the CSF 2.0 Subcategories in addition to the guidance provided in the Informative References.
CSF 2.0 Reference Tool	Access human and machine-readable versions of the Core (in JSON and Excel). You can also view and export portions of the Core using key search terms.

Additional Resources Include:

Community Profiles and Profile templates (help organizations put the CSF into practice)

Search tools (simplify and streamline as you look for specific information)

Concept papers (learn more about various CSF topics)

FAQs (see what others are asking and get answers to top questions)

Explore the suite of NIST's CSF 2.0 Resource Repository

NIST CSF 2.0:
RESOURCE & OVERVIEW GUIDE

NAVIGATING NIST's CSF 2.0 QUICK START GUIDES (QSG)

QSG Type	Description	Explore
Small Business (SMB)	Provides SMBs, specifically those who have modest or no cybersecurity plans in place, with considerations to kick-start their cybersecurity risk management strategy.	See the QSG
Creating and Using Organizational Profiles	Provides all organizations with considerations for creating and using Current and/or Target Profiles to implement the CSF 2.0.	See the QSG
Using the CSF Tiers	Explains how any organization can apply the CSF Tiers to Organizational Profiles to characterize the rigor of its cybersecurity risk governance and management practices.	See the QSG
Draft Cybersecurity Supply Chain Risk Management (C-SCRM)	Helps all organizations to become smart acquirers and suppliers of technology products and services by improving their C-SCRM processes.	See the QSG
Draft Enterprise Risk Management (ERM) Practitioners	Details how Enterprise Risk Management practitioners can utilize the outcomes provided in CSF 2.0 to improve organizational cybersecurity risk management.	See the QSG

…and more to follow in the future.

See the current online QSG repository

NIST CSF 2.0: RESOURCE & OVERVIEW GUIDE

GOVERN

The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.

Understand and assess specific cybersecurity needs. Determine your organization's unique risks and needs. Discuss the current and predicted risk environment and the amount of risk your organization is willing to accept. Seek input and ideas from across the organization. Understand what has worked or not worked well in the past and discuss it openly.

Develop a tailored cybersecurity risk strategy. This should be based on your organization's specific cybersecurity objectives, the risk environment, and lessons learned from the past — and from others. Manage, update, and discuss the strategy at regular intervals. Roles and responsibilities should be clear.

Establish defined risk management policies. Policies should be approved by management and should be organization-wide, repeatable, and recurring, and should align with the current cybersecurity threat environment, risks (which will change over time), and mission objectives. Embed policies in company culture to help drive and inspire the ability to make informed decisions. Account for legal, regulatory, and contractual obligations.

Develop and communicate organizational cybersecurity practices. These must be straightforward and communicated regularly. They should reflect the application of risk management to changes in mission or business requirements, threats, and overall technical landscape. Document practices and share them with room for feedback and the agility to change course.

Establish and monitor cybersecurity supply chain risk management. Establish strategy, policy, and roles and responsibilities — including for overseeing suppliers, customers, and partners. Incorporate requirements into contracts. Involve partners and suppliers in planning, response, and recovery.

Implement continuous oversight and checkpoints. Analyze risks at regular intervals and monitor them continuously (just as you would with financial risks).

IDENTIFY

The organization's current cybersecurity risks are understood.

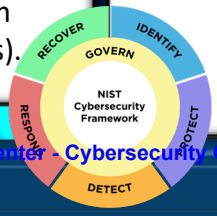
Identify critical business processes and assets. Consider which of your organization's activities absolutely must continue to be viable. For example, this could be maintaining a website to retrieve payments, securely protecting customer/patient information, or ensuring that the information critical to your organization remains accessible and accurate.

Maintain inventories of hardware, software, services, and systems. Know what computers and software your organization uses — including services provided by suppliers — because these are frequently the entry points of malicious actors. This inventory could be as simple as a spreadsheet. Consider including owned, leased, and employees' personal devices and apps.

Document information flows. Consider what type of information your organization collects and uses (and where the data are located and how they are used), especially when contracts and external partners are involved.

Identify threats, vulnerabilities, and risk to assets. Informed by knowledge of internal and external threats, risks should be identified, assessed, and documented. Examples of ways to document them include risk registers – repositories of risk information, including data about risks over time. Ensure risk responses are identified, prioritized, and executed, and that results are monitored.

Lessons learned are used to identify improvements. When conducting day-to-day business operations, it is important to identify ways to further refine or enhance performance, including opportunities to better manage and reduce cybersecurity risks. This requires purposeful effort by your organization at all levels. If there is an incident, assess what happened. Prepare an after-action report that documents the incident, the response, recovery actions taken, and lessons learned.



NIST CSF 2.0: RESOURCE & OVERVIEW GUIDE

PROTECT

Safeguards to manage the organization's cybersecurity risks are used.

Manage access. Create unique accounts for employees and ensure users only have access to necessary resources. Authenticate users before they are granted access to information, computers, and applications. Manage and track physical access to facilities/devices.

Train users. Regularly train employees to ensure they are aware of cybersecurity policies and procedures and that they have the knowledge and skills to perform general and specific tasks; explain how to recognize common attacks and report suspicious activity. Certain roles may require extra training.

Protect and monitor your devices. Consider using endpoint security products. Apply uniform configurations to devices and control changes to device configurations. Disable services or features that don't support mission functions. Configure systems and services to generate log records. Ensure devices are disposed of securely.

Protect sensitive data. Ensure sensitive stored or transmitted data are protected by encryption. Consider utilizing integrity checking so only approved changes are made to data. Securely delete and/or destroy data when no longer needed or required.

Manage and maintain software. Regularly update operating systems and applications; enable automatic updates. Replace end-of-life software with supported versions. Consider using software tools to scan devices for additional vulnerabilities and remediate them.

Conduct regular backups. Back up data at agreed-upon schedules or use built-in backup capabilities; software and cloud solutions can automate this process. Keep at least one frequently backed-up set of data offline to protect it against ransomware. Test to ensure that backed-up data can be successfully restored to systems.

DETECT

Possible cybersecurity attacks and compromises are found and analyzed.

Monitor networks, systems, and facilities continuously to find potentially adverse events. Develop and test processes and procedures for detecting indicators of a cybersecurity incident on the network and in the physical environment. Collect log information from multiple organizational sources to assist in detecting unauthorized activity.

Determine and analyze the estimated impact and scope of adverse events. If a cybersecurity event is detected, your organization should work quickly and thoroughly to understand the impact of the incident. Understanding details regarding any cybersecurity incidents will help inform the response.

Provide information on adverse events to authorized staff and tools. When adverse events are detected, provide information about the event internally to authorized personnel to ensure appropriate incident response actions are taken.

NIST CSF 2.0: RESOURCE & OVERVIEW GUIDE

RESPOND

Actions regarding a detected cybersecurity incident are taken.

Execute an incident response plan once an incident is declared, in coordination with relevant third parties. To properly execute an incident response plan, ensure everyone knows their responsibilities; this includes understanding any requirements (e.g., regulatory, legal reporting, and information sharing).

Categorize and prioritize incidents and escalate or elevate as needed. Analyze what has been taking place, determine the root cause of the incident, and prioritize which incidents require attention first from your organization. Communicate this prioritization to your team and ensure everyone understands who information should be communicated to regarding a prioritized incident when it occurs.

Collect incident data and preserve its integrity and provenance. Collecting information in a safe manner will help in your organization's response to an incident. Ensure that data are still secure after the incident to maintain your organization's reputation and trust from stakeholders. Storing this information in a safe manner can also help inform updated and future response plans to be even more effective.

Notify internal and external stakeholders of any incidents and share incident information with them — following policies set by your organization. Securely share information consistent with response plans and information-sharing agreements. Notify business partners and customers of incidents in accordance with contractual requirements.

Contain and eradicate incidents. Executing a developed and tested response plan will help your organization contain the effects of an incident and eradicate it. Meaningful coordination and communication with stakeholders can result in a more effective response and mitigation of the incident.

RECOVER

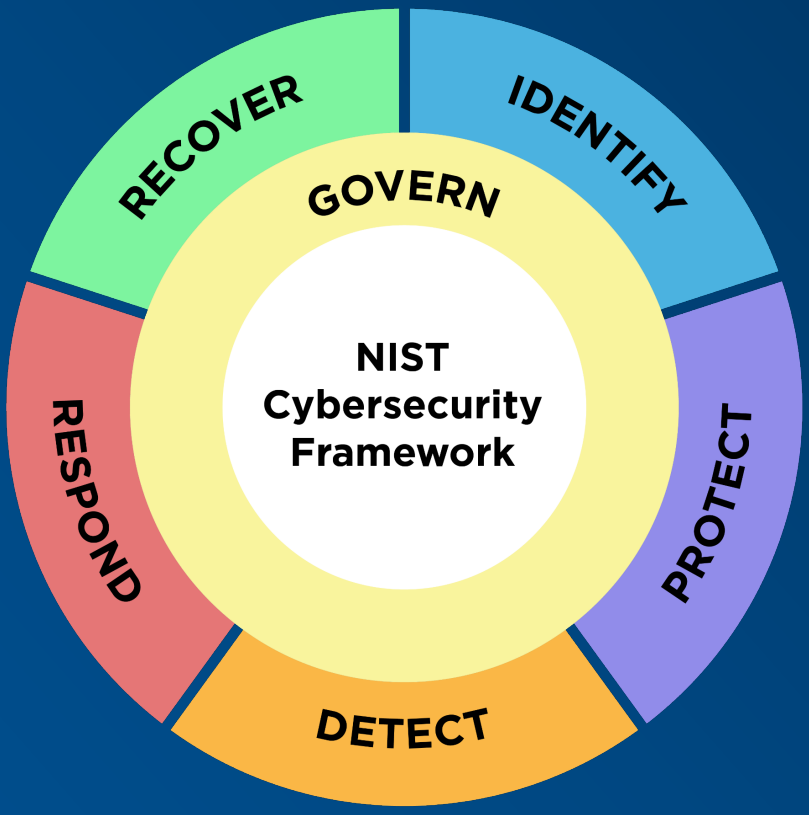
Assets and operations affected by a cybersecurity incident are restored.

Understand roles and responsibilities. Understand who, within and outside your business, has recovery responsibilities. Know who has access and authority to make decisions to carry out your response efforts on behalf of the business.

Execute your recovery plan. Ensure operational availability of affected systems and services; and prioritize and perform recovery tasks.

Double-check your work. It is important to ensure the integrity of backups and other recovery assets before using them to resume regular business operations.

Communicate with internal and external stakeholders. Carefully account for what, how, and when information will be shared with various stakeholders so that all interested parties receive the information they need, but no inappropriate information is shared. Communicate to your staff any lessons learned and revisions to processes, procedures, and technologies (following policies already set by the organization). This is a good time to train, or retrain, staff on cybersecurity best practices.



U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology