CRYPTONITE NXT

NIST 800-171 Achieving Mandatory Compliance

A Cryptonite Special Report

The smarter way to defend your network

Contents

Notice 3

Executive Summary 4

The Origin of CUI Terminology 5

Pivot Point - The Cyber Attack on OPM 5

NIST 800-171 and CryptoniteNXT 6

- 3.1 ACCESS CONTROL 6
- 3.2 AWARENESS AND TRAINING 8
- 3.3 AUDIT AND ACCOUNTABILITY 8
- 3.4 CONFIGURATION MANAGEMENT 9
- 3.5 IDENTIFICATION AND AUTHENTICATION 10
- 3.6 INCIDENT RESPONSE 10
- 3.7 MAINTENANCE 11
- 3.8 MEDIA PROTECTION 11
- 3.9 PERSONNEL SECURITY 12
- 3.10 PHYSICAL PROTECTION 12
- 3.11 RISK ASSESSMENT 12
- 3.12 SECURITY ASSESSMENT 12
- 3.13 SYSTEM AND COMMUNICATIONS PROTECTION 13
- 3.14 SYSTEM AND INFORMATION INTEGRITY 14

Recommended Actions 15

Appendix A - CUI Defined by Category 16

Published: 1 October, 2017 | This is a publication of Cryptonite, LLC - Labs and Research Group

Notice

Cryptonite, LLC publications are made available for information purposes only. At the time of publication, all information referenced in this publication is as current and accurate as we could determine. Any additional developments or research, since publication, will not be reflected in this report. Please note that this publication may be changed, improved, or updated without notice. Cryptonite, LLC is not responsible for any errors or omissions in the content of this report or for damages arising from the use of this report under any circumstances.

Executive Summary

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information (CUI) in Non Federal Information Systems and Organizations" requires that every government contractor have a plan in place to apply the specified security controls by December 31, 2017.

Government contractors with access to government data or federal information systems that are accessing CUI as part of their contract performance are now specifically obligated to protect per the specifications of NIST 800-171. Your data may not be labeled as CUI but it may still fall into the definition of CUI and will therefore require compliance. CUI may include project management, technical writing, system development, and consulting data, other non-classified data records, and more in support of federal contracts.

If you are bidding on new contracts, you will not be competitive nor will your bid be responsive if you are not compliant with NIST 800-171. If your firm is audited and found to have not properly implemented NIST 800-171, the penalties can be severe. These penalties may include contractual, administrative, civil, and in some cases criminal penalties. These penalties can directly impact ongoing and future contracts, the reputation of the firm and specific complicit individuals. Consequences may include, but are not limited to, breach of contract damages, liquidated damages, false claims act damages, suspension, disbarment, and termination for default. By signing a contract and submitting invoices your organization agrees to comply with all clauses within the contract.

The compliance process starts with a review of the requirements to determine policy and process requirements and their implementation requirements using IT resources, other IT configuration requirements, and any additional hardware or software you will require. You must understand what requirements you can meet using in-house compliance and IT personnel, and which require additional outside expertise.

Finally, you must develop and document a plan of action and the necessary milestones to implement the requirements by December 31, 2017. Most of the requirements in NIST 800-171 focus on policy, process, and the secure configuration of IT assets. Some of the requirements may require additional security related hardware and software.

Moving target cyber defense (MTD) and fine-grained micro-segmentation can help meet many of the requirements of NIST 800-171 and the challenges present in the current cyber threat environment. We will share how these technologies can help meet these requirements and how they address common and unprotected vulnerabilities within your organization.

The Origin of CUI Terminology

In 2010 the White House issued executive order 13556, which specified the control of unclassified information. The goal, in part, was to eliminate the inconsistency across various government agencies caused by widely varying terminology. There were over 100 different designations for unclassified data requiring some level of protection. Examples of this confusing terminology included: sensitive but unclassified (SBU), for official use only (FOUO), law enforcement sensitive (LES), sensitive homeland security information, sensitive security information (SSI), critical infrastructure information (CII), protected as restricted data (PARD), limited distribution, proprietary, originator controlled, and many more. The new terminology using CUI was intended to identify the many categories of information that need protection due to privacy requirements, security concerns, confidential contractor or business data, or that might be highly sensitive with respect to a law enforcement investigation.

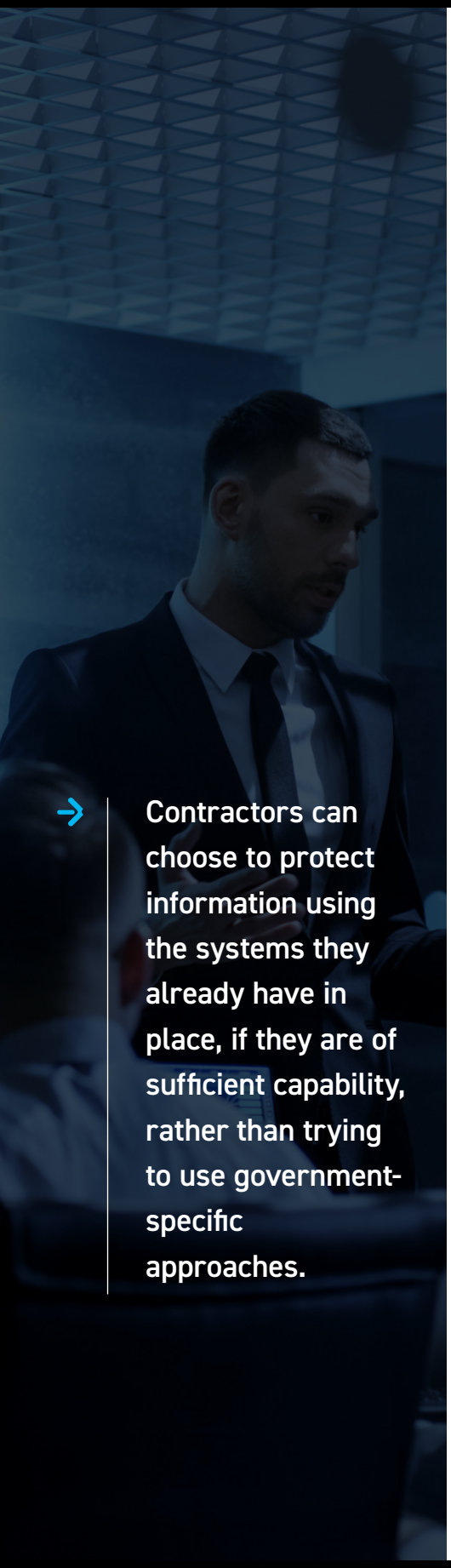
The National Archives and Records Administration is charged with defining standards for unclassified data and overseeing agency compliance. CUI is considered any potentially sensitive yet unclassified data that requires controls for proper safeguarding and distribution. Each agency must create an assignment of CUI categories for sensitive, unclassified information.

Pivot Point - The Cyberattack on OPM

Cybersecurity concerns were mounting globally in the wake of continued highly visible attacks on both commercial and government institutions. The issue over protecting unclassified but sensitive data was brought to a crescendo within the U.S. federal government by the massive cyberattacks on the US Office of Personnel Management (OPM), discovered in 2015. In the first cyberattack and data breach discovered by OPM in April 2015, personal information of 4.2 million current and former federal government employees was exfiltrated. In the second cyberattack and data breach, uncovered in June 2015, the data associated with the background investigations of both current, former, and prospective federal employees and contractors was exfiltrated. These attacks also included millions of digital images of the government employees' fingerprints.[1]

The Department of Defense (DOD), General Services Administration (GSA), and National Aeronautics and Space Administration (NASA) moved rapidly to publish a rule that requires federal government contractors to implement cybersecurity controls to protect corporate information systems effective June 15, 2016. The systems are to be protected with control requirements based on security requirements published in NIST 800-171.

1 These attacks on OPM were attributed to China's People's LIberation Army secret unit 61398. It was believed at that time, per a previous report published by Mandiant, that more than 1,000 servers and a special fiber optic communication infrastructure, provided by state-owned China Telecom, were being used by unit 61398 to promulgate this attack and many others. https://www.cbsnews.com/news/china-military-unit-behind-many-hacking-attacks-on-us-cybersecurity-firm-says/



Contractors can choose to protect information using the systems they already have in place, if they are of sufficient capability, rather than trying to use government-specific approaches.

NIST 800-171 and CryptoniteNXT

NIST 800-171 is applicable to internal contractor information systems and provides a standardized set of security requirements for non federal organizations to be in compliance with to ensure the correct implementation of CUI safeguards. Most of the NIST 800-171 controls are about best practices concerning policies and technology implementation.

NIST 800-171 publishes over one hundred controls categorized into 14 control families. NIST SP 800-171 allows nonfederal organizations more flexibility in defining how requirements are implemented. Contractors can choose to protect information using the systems they already have in place, if they are of sufficient capability, rather than trying to use government-specific approaches.

The CryptoniteNXT platform brings capabilities in moving target cyber defense (MTD) and fine-grained micro-segmentation which can provide positive impact in many of the 14 control families. The specific potential impact of CryptoniteNXT is documented below and highlighted in light blue where applicable. Derived security requirements for which CryptoniteNXT does not provide any impact are not listed below.

3.1 ACCESS CONTROL

Basic Security Requirements:

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

CryptoniteNXT support: *CryptoniteNXT micro-segmentation restricts authenticated user movement and access to resources within the network by policy. Users that must still login to systems, web applications and other applications need their own credentials. CryptoniteNXT moving target cyber defense (MTD) further restricts access by disabling reconnaissance within the network.*

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

CryptoniteNXT support: *CryptoniteNXT micro-segmentation restricts user movement and access to resources, such as information systems, within the network by policy. Users that must still login to systems, web applications and other applications need their own credentials.*

Derived Security Requirements:

3.1.14 Route remote access via managed access control points.

CryptoniteNXT support: *CryptoniteNXT provides support for strong access control point technology such as HPE Aruba Networks' wireless access control points. Strong authentication then enables the implementation of policy by CryptoniteNXT micro-segmentation, to strictly manage and control the users that come in through these wireless control points. CryptoniteNXT also applies segmentation policy to VPN based users that are authenticated into a protected network.*

3.1.16 Authorize wireless access prior to allowing such connections.

CryptoniteNXT support: *CryptoniteNXT provides support for strong access control point technology such as HPE Aruba Networks' wireless access control points. Strong authentication then enables the implementation of policy by CryptoniteNXT micro-segmentation, to strictly manage and control the users that come in through these wireless control points.*

3.1.18 Control connection of mobile devices.

CryptoniteNXT support: *CryptoniteNXT provides support for strong access control point technology such as HPE Aruba Networks' wireless access control points. Strong authentication then enables the implementation of policy by CryptoniteNXT micro-segmentation, to strictly manage and control the users that come in through these wireless control points.*

3.2 AWARENESS AND TRAINING

Basic Security Requirements:

3.2.1 Ensure that managers, systems administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information systems.

3.2.2 Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities. Provide security awareness training on recognizing and reporting potential indicators of insider threat.

3.3 AUDIT AND ACCOUNTABILITY

Basic Security Requirements:

3.3.1 Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.

CryptoniteNXT support: *CryptoniteNXT provides support for audit records using tools such as Splunk which provides traffic analysis for all communications that we are protecting. Specific alerts record out of bounds policy and access to IP addresses that are out of range. These high value alerts contain source IP and username to aide investigation. For network authentication, CryptoniteNXT provides all of the information provided.*

3.3.2 Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

CryptoniteNXT support: *Specific alerts from CryptoniteNXT record out of bounds policy and access to IP addresses that are out of range. These high value alerts contain source IP and username to aide investigation and hold malicious insiders accountable for their actions.*

3.4 CONFIGURATION MANAGEMENT

Basic Security Requirements:

3.4.1 Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

CryptoniteNXT support: *CryptoniteNXT prevents non-inventoried systems from connecting to the network. This ensures inventory correctness and control of access. We also automate the identification and onboarding of non-inventoried devices. This information is logged, and visible in tools like Splunk.*

3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational information systems.

Derived Security Requirements:

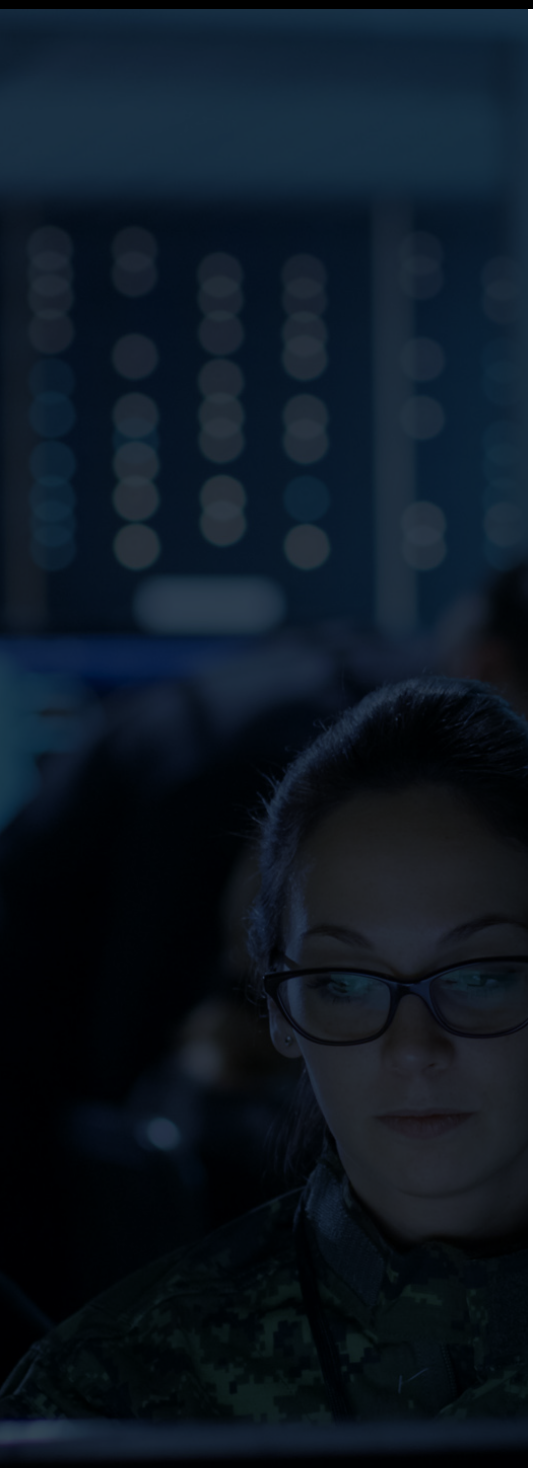
3.4.6 Employ the principle of least functionality by configuring the information system to provide only essential capabilities.

CryptoniteNXT support: *CryptoniteNXT also enforces logical access restrictions through the best practice of Zero Trust. Zero Trust network best practices require minimizing access to resources and visibility within the network to the absolute minimal subset each account needs to perform the requirements of their job - no more. Hence users are limited to access in support of only essential capabilities.*

3.4.7 Restrict, disable, and prevent the use of non essential programs, functions, ports, protocols, and services.

CryptoniteNXT support: *CryptoniteNXT allows the restriction of ports, protocols, and services through the use of micro-segmentation. We restrict network access, not endpoint devices.*

CryptoniteNXT MTD places attackers or unauthorized personnel in an environment where the primary network protocol, TCP/IP, no longer provides complete access for view and enumeration of addresses within the network - they are not accessible. Therefore, they can no longer be used to map out and enumerate an attack. Even if the attacker had the TCP/IP address prior to the installation of the CryptoniteNXT appliance, they can no longer use that address to successfully navigate the network. It will no longer work. Lateral east-west movement in the network is similarly restricted and limited by role and policy as implemented by micro-segmentation.



3.5 IDENTIFICATION AND AUTHENTICATION

Basic Security Requirements:

3.5.1 Identify information system users, processes acting on behalf of users, or devices.

CryptoniteNXT support: CryptoniteNXT identifies all of these users and requires 2 factor authentication.

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

CryptoniteNXT support: CryptoniteNXT supports existing network authentication mechanisms as well as our own which is based upon the Time based One Time Password algorithm (TOTP). Once authenticated into a protected network, policy is assigned to users and their devices to allow access to organizational information systems.

Derived Security Requirements:

3.5.3. Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

CryptoniteNXT support: *The CryptoniteNXT appliance requires login using two (2) factor authentication and seamlessly integrates to other network based platforms (e.g. Radius) for purposes of multifactor authentication.*

3.6 INCIDENT RESPONSE

Basic Security Requirements:

3.6.1 Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.

CryptoniteNXT support: *CryptoniteNXT provides for pre-planning in the event of an incident. In the event of an incident, that policy can be immediately activated organization-wide with a single click.*

3.6.2 Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization.

3.7 MAINTENANCE

Basic Security Requirements:

3.7.1 Perform maintenance on organizational information systems.

CryptoniteNXT support: *CryptoniteNXT provides a strong 2nd line of defense to help mitigate critical vulnerabilities exposed due to missing updates (and patches). Cryptonite MTD obfuscates the location and details of network vulnerabilities so that the timing of security updates are not as critical.*

3.7.2 Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

3.8 MEDIA PROTECTION

Basic Security Requirements:

3.8.1 Protect (i.e., physically control and securely store) information system media containing CUI , both paper and digital.

3.8.2 Limit access to CUI on information system media to authorized users.

3.8.3 Sanitize or destroy information system media containing CUI before disposal or release for reuse.

3.9 PERSONNEL SECURITY

Basic Security Requirements:

3.9.1 Screen individuals prior to authorizing access to information systems containing CUI.

3.9.2 Ensure that CUI and information systems containing CUI are protected during and after personnel actions such as terminations and transfers

3.10 PHYSICAL PROTECTION

Basic Security Requirements:

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

3.10.2 Protect and monitor the physical facility and support infrastructure for those information systems.

3.11 RISK ASSESSMENT

Basic Security Requirements:

3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of CUI.

3.12 SECURITY ASSESSMENT

Basic Security Requirements:

3.12.1 Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.

3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.

3.12.3 Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

3.13 SYSTEM AND COMMUNICATIONS PROTECTION

Basic Security Requirements:

3.13.1 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.

CryptoniteNXT support: *The CryptoniteNXT appliance uses micro-segmentation to enforce policy that defines internal boundaries within the network and access of individuals to information systems both inside and outside of those defined boundaries. Micro-segmentation protects against unauthorized access to any server by physically limiting access to the server's TCP/IP addresses by policy. CryptoniteNXT also provides additional monitoring through logging and integration to products such as Splunk.*

3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

Derived System Requirements:

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

CryptoniteNXT support: *CryptoniteNXT micro-segmentation creates logical separation within internal networks based upon policy. This policy usually defines the minimum resource access required for each individual to perform the requirements of their position.*

3.13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

CryptoniteNXT support: CryptoniteNXT micro-segmentation can implement a strategy of "deny all" and "permit" by exception. The CryptoniteNXT moving target cyber defense (MTD) denies all network reconnaissance traffic.

3.13.15. Protect the authenticity of communications sessions.

CryptoniteNXT support: *The CryptoniteNXT appliance also stops spoofing and man-in-the-middle attacks, which helps protect the authenticity of communications sessions. CryptoniteNXT cryptographically verifies and enforces the identity of the sender, as well as the integrity of the packet, end to end. In addition, CryptoniteNXT prevents attacks against network services, protocols, and network infrastructure.*

3.14 SYSTEM AND INFORMATION INTEGRITY

Basic Security Requirements:

3.14.1 Identify, report, and correct information and information system flaws in a timely manner.

3.14.2 Provide protection from malicious code at appropriate locations within organizational information systems.

CryptoniteNXT support: *CryptoniteNXT micro-segmentation stops malicious attacks and related attacker tools, almost all of which rely on the utilization of TCP/IP addresses and network access. These resources are unavailable, hence the malicious code can neither propagate nor execute beyond the initial point of infection.*

3.14.3 Monitor information system security alerts and advisories and take appropriate actions in response.

Derived Security Requirements:

3.14.6 Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

CryptoniteNXT support: *The CryptoniteNXT appliance monitors all network traffic within the networks it is configured to protect. Violations of policy, which include the use of scanning (reconnaissance) tools, and attempted violations of micro-segmentation and moving target cyber defense (MTD) are logged and reported to the SIEM.*

Recommended Actions

Contractors who own or operate information systems that process (store in any way, communicate, transmit) any federal contract information should:

- Review all of the security controls specified within NIST 800-171.
- Review your security implementation to ensure you meet specified protection requirements and that you address the current and growing wide range of cyberthreats.
- Utilize the U.S. Department of Homeland Security CSET® tool - https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET.
- Conduct a careful and detailed assessment and risk analysis.
- Develop an IT Security plan to immediately address gaps to meet and maintain compliance requirements by 31 December 2017.
- Evaluate how and where a Zero Trust network infrastructure using CryptoniteNXT can help your organization meet many of the key requirements of NIST 800-171.

Appendix A - CUI Defined by Category

Controlled Unclassified Information is defined by Categories and Category Descriptions in the tables below:

CATEGORY	CATEGORY DESCRIPTION
Agriculture	Information related to the agricultural operation, farming or conservation practices, or the actual land of an agricultural producer or landowner.
Controlled Technical Information	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 is to be marked with one of the distribution statements B through F, in accordance with Department of Defense Instruction 5230.24, "Distribution Statements of Technical Documents." The term does not include information that is lawfully publicly available without restrictions. "Technical Information" means technical data or computer software, as those terms are defined in Defense Federal Acquisition Regulation Supplement clause 252.227-7013, "Rights in Technical Data - Noncommercial Items" (48 CFR 252.227-7013). 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.
Critical Infrastructure **Subcategories**: Ammonium Nitrate Chemical-terrorism Vulnerability Information Critical Energy Infrastructure Information DoD Critical Infrastructure Security Information Physical Security Protected Critical Infrastructure Information Water Assessments	Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any Federal, State, regional, territorial, or local jurisdiction.

Emergency Management	Related to information concerning the continuity of executive branch operations during all-hazards emergencies or other situations that may disrupt normal operations.
Export Control **Subcategories**: Research	Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. To include dual use items; items identified in export administration regulations, international traffic in arms regulations and the munitions list; license applications; and sensitive nuclear technology information.
Financial **Subcategories**: Bank Secrecy Budget Comptroller General Electronic Funds Transfer Federal Housing Finance Non-Public Information International Financial Institutions Mergers Net Worth Retirement	Related to the duties, transactions, or otherwise falling under the purview of financial institutions or United States Government fiscal functions. Uses may include, but are not limited to, customer information held by a financial institution.
Geodetic Product Information	Related to imagery, imagery intelligence, or geospatial information.
Immigration Controlled at the Subcategory level only. **Subcategories**: Asylee Battered Spouse or Child Permanent Resident Status Status Adjustment Temporary Protected Status Victims of Human Trafficking Visas	Related to admission of non-US citizens into the United States and applications for temporary and permanent residency.

Information Systems Vulnerability Information	Related to information that if not protected, could result in adverse effects to information systems. Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Intelligence **Subcategories**: Financial Records Foreign Intelligence Surveillance Act Foreign Intelligence Surveillance Act Business Records Internal Data National Security Letter Terrorist Screening	Related to intelligence activities, sources, or methods.
International Agreements	Information provided by, otherwise made available by, or produced in cooperation with, a foreign government or international organization that requires protection pursuant to an existing treaty, agreement, bilateral exchange or other obligation under the requirements stipulated in 10 USC 130c(b), when not subject to classification under Executive Order 13526. Title 10 USC 130c(b) may exempt this class of foreign government information from the safeguard provisions otherwise required by Executive Order 13526. Per Title 10 USC 130c(h) the following national security officials are the only ones defined by statute as able to determine such information requires control: (A) The Secretary of Defense, with respect to information of concern to the Department of Defense. (B) The Secretary of Homeland Security, with respect to information of concern to the Coast Guard, as determined by the Secretary, but only while the Coast Guard is not operating as a service in the Navy. (C) The Secretary of Energy, with respect to information concerning the national security programs of the Department of Energy, as determined by the Secretary.

Law Enforcement **Subcategories:** Campaign Funds Committed Person Communications Controlled Substances Criminal History Records Information DNA Financial Records Informant Investigation Juvenile National Security Letter Pen Register/Trap & Trace Reward Sex Crime Victim Terrorist Screening Whistleblower Identity	Related to techniques and procedures for law enforcement operations, investigations, prosecutions, or enforcement actions.
Legal Controlled at the Subcategory level only. **Subcategories**: Administrative Proceedings Child Pornography Child Victim/Witness Collective Bargaining Federal Grand Jury Presentence Report Prior Arrest Privilege Protective Order Victim Witness Protection	Information related to proceedings in judicial or quasi-judicial settings.

Natural and Cultural Resources Controlled at the Subcategory level only. **Subcategories**: Archaeological Resources Historic Properties National Park System Resources	Related to information concerning natural and cultural resources.
North Atlantic Treaty Organization (NATO) Controlled at the Subcategory level only. **Subcategories**: NATO Restricted NATO Unclassified	Related to information generated by North Atlantic Treaty Organization (NATO) member countries under the North Atlantic Treaty international agreement, signed on April 4, 1949.
Nuclear **Subcategories**: Naval Nuclear Propulsion Information Recommendation Material Safeguards Information Security-Related Information Unclassified Controlled Nuclear Information - Defense Unclassified Controlled Nuclear Information - Energy	Related to protection of information concerning nuclear reactors, materials, or security.
Patent Controlled at the Subcategory level only. **Subcategories**: Application Invention Secrecy Orders	Patent is a property right granted by the Government of the United States of America to an inventor "to exclude others from making, using, offering for sale, or selling the invention throughout the United States or importing the invention into the United States" for a limited time in exchange for public disclosure of the invention when the patent is granted.

Privacy **Subcategories**: Contract Use Death Records Genetic Information Health Information Inspector General Military Personnel Student Records	Refers to personal information, or, in some cases, "personally identifiable information," as defined in OMB M-17-12, or "means of identification" as defined in 18 USC 1028(d)(7).
Procurement and Acquisition **Subcategories**: Small Business Research and Technology Source Selection	Material and information relating to, or associated with, the acquisition and procurement of goods and services, including but not limited to, cost or pricing data, contract information, indirect costs and direct labor rates.
Proprietary Business Information **Subcategories**: Manufacturer Ocean Common Carrier and Marine Terminal Operator Agreements Ocean Common Carrier Service Contracts Postal System for Award Management	Material and information relating to, or associated with, a company's products, business, or activities, including but not limited to financial information; data or statements; trade secrets; product research and development; existing and future product designs and performance specifications.

SAFETY Act Information	Defined as "SAFETY Act Confidential Information" in 6 CFR Part 25, the regulations implementing the Support Anti-terrorism by Fostering Effective Technologies Act of 2002, SAFETY Act Information includes any and all information and data voluntarily submitted to the Department of Homeland Security under this part (including Applications, Pre-Applications, other forms, supporting documents and other materials relating to any of the foregoing, and responses to requests for additional information), including, but not limited to, inventions, devices, Technology, know-how, designs, copyrighted information, trade secrets, confidential business information, analyses, test and evaluation results, manuals, videotapes, contracts, letters, facsimile transmissions, electronic mail and other correspondence, financial information and projections, actuarial calculations, liability estimates, insurance quotations, and business and marketing plans.
Statistical **Subcategories**: Census Investment Survey Pesticide Producer Survey	Refers to information collected by a Federal statistical agency, unit, or program for statistical purposes or used for statistical activities; under law, regulation, or Government-wide policy such 'Statistical' CUI requires: (1) protection from unauthorized disclosure; (2) special handling safeguards; and/or (3) prescribed limits on access or dissemination.
Tax **Subcategories**: Convention	Related to a compulsory contribution to government revenue involving information regarding returns or taxpayers.
Transportation Controlled at the Subcategory level only. **Subcategories**: Railroad Safety Analysis Records Sensitive Security Information	Related to any mode of travel or conveyance by air, land, or waterway.

For More Information

To learn more about Cryptonite, LLC and CryptoniteNXT, please email **info@cryptonitenxt.com**

This document is current as of the initial date of publication and may be changed by Cryptonite at any time.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NONINFRINGEMENT.

Cryptonite products are warranted according to the terms and conditions of the agreements under which they are provided. The client is responsible for ensuring compliance with laws and regulations applicable to it. Cryptonite does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access.

CRYPTONITE DOES NOT WARRANT THAT ITS PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

About Cryptonite, LLC

Cryptonite is a leader in moving target cyber defense. CryptoniteNXT enables any network to actively shield itself from cyber-attacks by preventing all attacker reconnaissance and lateral movement. Patent pending moving target cyber defense and micro-segmentation technologies protect enterprise networks from an advanced cyber attacker, insider threats and ransomware. The Cryptonite customer base includes leading commercial and government customers around the world. Learn more at **www.cryptonitenxt.com.**