Cyber Security Capstone Research Project Reports

Department of Computing and Information Sciences

4-27-2017

Cybersecurity Compliance and DoD Contractors

Ernie Magnotti
Valparaiso University

Cybersecurity, Compliance & DoD Contractors

Ernie Magnotti

CYB 692: Capstone Project

4/27/2017

Cybersecurity Compliance & DoD Contractors

Table of Contents

Table of Figures

Introduction

“We Should Take Nothing for Granted”

President Dwight D. Eisenhower coined the phrase “military–industrial complex” (MIC) to describe the informal alliance between the U.S. military and the DoD contractors who supplies it. [1] Within this alliance, hundreds of billions of dollars are spent annually the enable the power of the U.S Military, the most dominant fighting force the world has ever seen.

When President Eisenhower used the phrase “Military Industrial Complex” in his farewell speech to the nation on January 17th, 1961, in was in the context of warning: “We should take nothing for granted. Only an alert and knowledgeable citizenry can compel the proper meshing of the huge industrial and military machinery of defense with our peaceful methods and goals so that security and liberty may prosper together.” [1] Eisenhower warned that the MIC should not become a self-perpetuator of wars creating more need for federal funding, creating more supply for waging war. Alternatively, when Eisenhower said, “we should take nothing for granted,” he may not have foreseen that one day our nations adversaries would be stealing valuable and sensitive military information through computer network connections that span the entire planet.

Sensitive but Unclassified Information

The phrase “sensitive but unclassified information” originated in the National Security Decision Directive (NSDD 145) signed by President Reagan on September 17th, 1984. The directive, titled “National Policy on Telecommunications and Automated Information Systems Security,” had far reaching significance in the world of computer security and was mandated to protect both classified and sensitive but unclassified information. The directive gave the NSA limited jurisdiction in the private sector. [2] Two years later, on October 29th, 1986, the National Telecommunications, and Information Systems Security Publication 2 (NTISSP 2) was published in an effort to clarify the meaning of sensitive but unclassified information while providing better interpretation of the protection requirements. The publication was titled the “National Policy on Protection of Sensitive but Unclassified Information in Federal Government Telecommunications and Automated Systems.” NTISSP 2 defined sensitive but unclassified information as “information the disclosure, loss, misuses, alteration, or destruction of which could adversely affect national security or other federal government interests. National security interests are those unclassified matters that relate to the national defense or foreign relations of the U.S. government.” NTISSP 2 applied to all government agencies and contactors. [2] However, the policy, which was drafted by Rear Adm. John M. Poindexter when he was National Security Advisor, was cancelled on March 19th, 1987 by Frank C. Carlucci, who succeeded Admiral Poindexter. [3]

NTISSP 2, essentially the safeguarding of sensitive but unclassified information, was cancelled for many reasons, but chief among them because it restricted competitiveness of U.S. private industry. The ideology that restricting capability versus safeguarding sensitive but unclassified information would survive another 25 years for DoD contractors.

MIC Federal Budget Impact and Market Scope

The U.S. became the most dominant force over the decades of the 20th and 21st centuries, through world wars, the Cold War, the threat of communism, and the threat of terrorism, by making defense spending the largest item in the annual discretionary budget of the Federal Government. The discretionary budget in 2016 was $1.15 trillion, and was about 25% of the total federal budget. The other 75% of the overall federal budget is the mandatory budget (Medicare, health care, social security, or interest on the national debt). [2] In 2016, defense budget was about 54% of the discretionary budget, which is about $622 billion. At $622 billion, the U.S. spends more on defense than the next seven countries in the world combined.[3] Having the world’s most powerful military has long been an esteemed value of most Americans, as exemplified over decades of U.S. leadership in the congress and the presidency.

The DoD awards approximately $300 billion annually in new contracts, and about 50% of the new contracts are awarded to the top 30 DoD contractors. [6] Yet, there were over 33,000 companies who contracted with the Department of Defense (DoD) in 2015. [6]

DoD contractors provide the military with items as large as aircraft carriers and as small as a small buoy. The MIC is a vast marketplace where the top companies (the medium and large DoD contractors) play consistent roles year after year (Lockheed supplies aircraft, Northrop Grumman supplies ships, General Dynamics supplies tanks). Small contactors make up 99% of the total number of defense contractors.

MIC Supply Chain Ecosystem and Sensitive but Unclassified Information

The 33,000 contractors who contracted with the DoD provides a reasonable idea of the market ecosystem. Certainly, not every DoD contractor stores sensitive but unclassified information. But it is highly likely that every contractor supplies to another DoD contractor that does. Obviously, the DoD itself stores and processes sensitive but unclassified information. There are at least 33,000 companies that store or are one vendor relationship away from an organization that stores sensitive but unclassified information.

During the Christmas season in 2013, the Target data breach showed how a company was vulnerable to a cyber-attack through its supply chain. “The attackers backed their way into Target's corporate network by compromising a third-party vendor. The number of vendors targeted is unknown. However, it only took one. That happened to be Fazio Mechanical, a refrigeration contractor.” [8]

The scope of the MIC supply chain ecosystem offers a vast attack surface for any target within the military industrial complex.

U.S. Taxpayer Expectations

U.S. taxpayers should expect that safeguarding sensitive but unclassified information be treated as a critical priority and that proportional efforts and expenditures are made by every company that is awarded contracts by the Department of Defense. Further, the U.S. Federal Government should ensure that a proper safeguarding standard is enforced and audited. Nothing should be taken for granted when it comes to cyber security in the MIC. The U.S. taxpayers have invested too much, and the U.S. national security is at stake.

Cyber Security in the Military Industrial Complex

The system at risk across the MIC can be divided into four areas of focus in terms of cyber security strategy: 1) Federal information systems containing data classified as secret or higher, 2) DoD contractor information systems containing data classified as secret or higher, 3) Federal information systems containing unclassified data, and 4) DoD contractor information systems containing unclassified data.

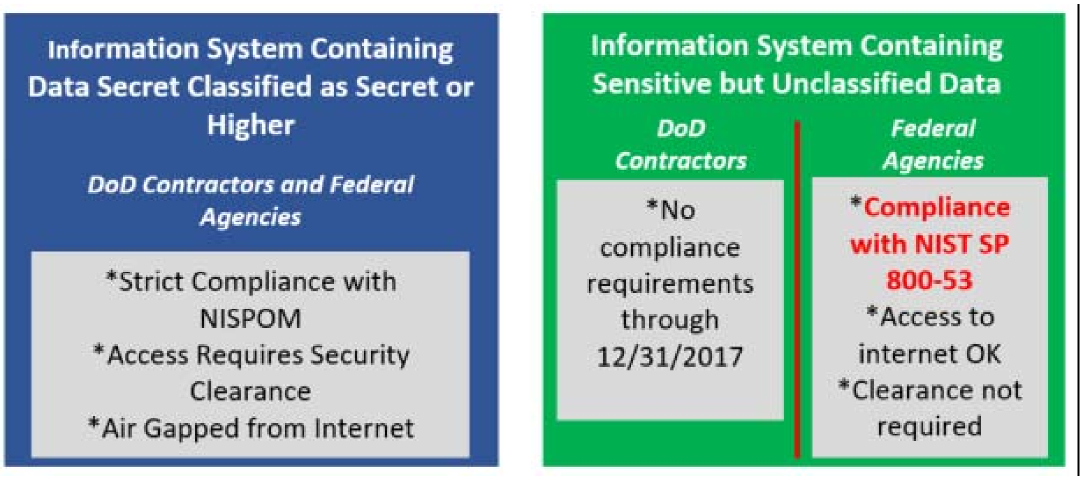

Information System Containing Data Secret Classified as Secret or Higher
DoD Contractors and Federal Agencies
*Strict Compliance with NISPOM
*Access Requires Security Clearance
*Air Gapped from Internet
Information System Containing Sensitive but Unclassified Data
DoD Contractors
*No compliance requirements through 12/31/2017
Federal Agencies
*Compliance with NIST SP 800-53
*Access to internet OK
*Clearance not required

Figure 1: Cyber Security in Military Industrial Complex before 12/31/2017

The National Industrial Security Program Operating Manual

Federal information systems and DoD contractor information systems containing classified data are managed by mature standards and processes that have been in place for more than two decades.

Executive Order 12829 was signed on January 6th, 1993 to establish “a National Industrial Security Program to safeguard Federal Government classified information that is released to contractors, licensees, and grantees of the United States Government.” [7] EO 12829 established the National Industrial Security Program (NISP), and the National Industrial Security Program Operating Manual (NISPOM). [8] NISP is specifically concerned with managing the needs of private industries access to classified information. Classified information requires a security clearance by both the individual and the contractor. Chapter 8 of the NISPOM describes the requirements and processes for managing information systems that store and process classified information. [9] Chapter 8 sets a high bar for information security. One of the key controls is that information systems are not allowed to be connected or routed to the internet in any way. The Defense Security Service (DSS) is the agency charged with oversight of the NISP, and they work closely with the cleared contractors to ensure that NISPOM security controls are continually maintained. When the DSS finds negligence in the cleared contractors implementation of the NISPOM, the contractor can lose accreditation, and consequently lose the DoD contract. Loss of a contract due to lack of compliance to the NISPOM is a high risk for cleared contractors, thus there is significant time, effort, resources and costs associated with NISPOM compliance.

The NISPOM is highly effective in protecting secret information and data. The operational complexities and costs for stealing classified information are higher for a hacker whose goal is to steal classified information versus unclassified information. The fact that classified information cannot be stored on a classified network is prohibited from having routed access to the internet (aka classified networks are air gapped from the internet) makes hacking classified networks very difficult. The NISPOM air gap control, in conjunction with the 149 pages of processes and procedures, assures appropriate protection of our DoD co-managed classified information. Cyber risk is thus managed effectively in both federal and DoD contractor information systems that contain classified data.

FISMA and NIST

In 2002, in response to 9/11 combined with increased concerns for cyber security, Congress passed the Federal Information System Management Act (FISMA). FISMA is the primary law that tells federal agencies how they must secure their unclassified IT systems. FISMA authorizes the National Institute of Standards and Technology (NIST) to develop security standards for IT systems that do not contain classified information. [10] NIST developed a Federal Information Processing Standard Publication called FIPS 200, which defines minimum security requirements. Then in February of 2005, NIST created Special Publication 800-53 to define specific cyber security controls for safeguarding unclassified federal information systems. NIST SP 800-53 has been revised 5 times since its introduction, and widely regarded as a benchmark standard to assess any organizations information system. But the federal law only requires that federal information systems comply with 800-53.

DoD Contractors Lacking Cyber Security Safeguarding Regulations

Although DoD contractors are required to comply with FISMA and FIPS 200 in principal, they are not required to comply with NIST SP 800-53 [13]. In fact, most defense contractors are not currently compelled to comply with any cyber security laws or standards on their unclassified networks. As mentioned in the Introduction, the ideology that restricting capability versus safeguarding sensitive but unclassified information would survived since the short lived NTISSP-2 was cancelled in 1987. It would not be until 2013 that safeguarding controls for sensitive but unclassified information would be reintroduced as a regulatory requirement for DoD contractors.

In the meantime, there is significant risk to sensitive but unclassified information in DoD contractor networks. While a DoD program may have a classified component, most program information is unclassified, for example: contract details, procurement information, engineering schedules, unclassified designs, manufacturing schedules, software development, persons with clearance working on the program, etc are typically unclassified. A DoD contractors unclassified network contains terabytes upon terabytes of sensitive and valuable DoD information and intellectual property.

This creates a paradoxical situation: The DoD wants to buy a complex widget so they put the complex widget out for bid to its contractors. DoD contractors compete with one another to supply the government with the complex widget at the lowest price, while still making a profit. The DoD contractor with the lowest price that meets specifications usually wins. But cyber security always adds up-front costs in terms of cyber security staff and tools. Costs are also added in terms of efficiency of business operations. For example, prohibiting local admin control of a regular user results in the user going through IT to make changes to their computer. This slows down the user and adds personnel needed to accomplish a task. DoD contractors must keep costs down and efficiencies up to win DoD contracts. This paradox is increasingly applicable as you go further down the scale of DoD contractor size. At the end of the day, a DoD contractor may not be motivated safeguard sensitive but unclassified information without regulatory requirements.

Motivations for Adversaries Targeting DoD Contractors

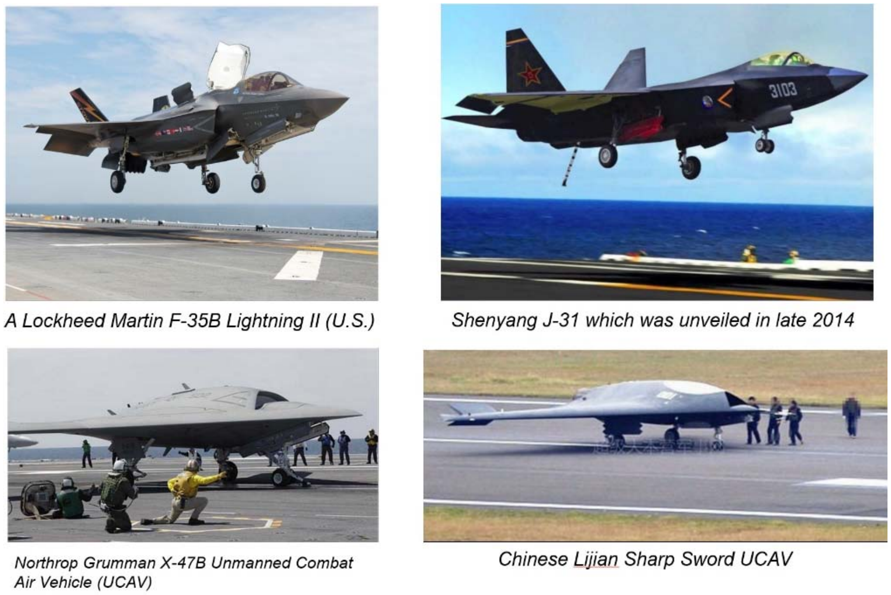
Since the Gulf War in 1991, the People's Liberation Army of China (PLA) has been undergoing a multi-decade effort to modernize its military to catch up to the United States. [12] As part of its modernization strategy, the PLA has systematically accessed sensitive unclassified data of other governments and defense companies including those in the U.S., as a strategic method to shortcut years of research and development.

Other countries, for example Russia, Iran and North Korea have also been active cyber attackers of U.S. networks. The motives for hacking are continually evolving. Russian hacking has been motivated by strategic intelligence gathering. Iran and North Korean has been hacking for the purpose of symbolic destruction towards enhancing the status of their political ideologies.

Example of U.S. Military Technology Being Hacked

In the context of superpower competition, China is unique due to the size and power of its economy. China is now the largest economy in the world when ranked by purchasing power parity. [13] Although many countries may have the offensive cyber capability to steal designs for a F-35B Joint Strike Fighter, China is the only rival with the economic resources to make their own copy.

What has taken years of research, development and defense spending for the US to maintain a strategic defensive advantage has unfortunately not resulted in a proportionately dominate position for the United States. More than any other adversary, China got the wake-up call in 1991, and began leveraging network vulnerabilities of DoD defense contractors, along with their rapidly growing economic power, China has significantly closed the gap with the US. [14]



A Lockheed Martin F-35B Lightning II (U.S.)

Shenyang J-31 which was unveiled in late 2014

Northrop Grumman X-47B Unmanned Combat Air Vehicle (UCAV)

Chinese Lijian Sharp Sword UCAV

Figure 2: Examples of Chinese Copies of F-35 and X-47B

It took Lockheed Martin nine years from the time it began developing the F-35 until the first production version was completed in 2006. [16] China hacked Lockheed Martin in 2009 and stole a huge amount of design and electronics data on the F-35. [17] The maiden flight for the Chinese knockoff J-31 took place in 2012, just three years later. [17]

Sensitive but Unclassified Rephrased as Controlled Unclassified Information

On November 4th, 2010, President Obama signed Executive Order 13556 mandating a Government-wide uniform program to identify and protect sensitive but unclassified information. EO 13556 was intended to align agency specific policies, procedures and markings for safeguarding and control. The executive order established a program for managing sensitive but unclassified information, and established a new reference term called Controlled Unclassified Information (CUI), replacing the term Sensitive but Unclassified. CUI categories and subcategories would serve as exclusive designations for identifying unclassified information throughout the executive branch that required safeguarding and dissemination controls.

EO 13556 established that the National Archives and Records Administration (NARA) would serve as the Executive Agent to implement the executive order and oversee agency actions to ensure compliance. The principal set of rules and regulations issued by federal agencies regarding national defense fall under Title 32 of the Code of Federal Regulations. 32 CFR 2002, established the following authorities over CUI: *“As the Federal Government's Executive Agent (EA) for Controlled Unclassified Information (CUI), the National Archives and Records Administration (NARA), through its Information Security Oversight Office (ISOO), oversees the Federal Government-wide CUI Program. As part of that responsibility, ISOO is issuing this rule to establish policy for agencies on designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI, self-inspection and oversight requirements, and other facets of the*

Program. The rule affects Federal executive branch agencies that handle CUI and all organizations (sources) that handle, possess, use, share, or receive CUI—or which operate, use, or have access to Federal information and information systems on behalf of an agency.” [25]

The National Archives created 23 categories for CUI, which are shown in the table below:

National Archives Categories of Controlled Unclassified Information		
Agriculture	Intelligence	Procurement and Acquisition
Critical Infrastructure	International Agreements	Proprietary Business Information
Emergency Management	Law Enforcement	SAFTEY Act Information
Export Control	Legal	Statistical
Financial	NATO	Tax
Geoditic	Nuclear	Transportation
Immigration	Patent	Controlled Technical Information
Information Systems Vulnerability	Privacy	

Figure 3: National Archives Categories of Controlled Unclassified Information

Controlled Technical Information

The Controlled Technical Information (CTI) category is the key that connects DoD contractor’s unclassified networks to Executive Order 13556 and is broad category that will potentially impact all contractors (Note that DoD contractors are also concerned with Export Control and Nuclear categories, but safeguarding rules for these existed for before the EO 13556, and only impact a small percentage of contractors).

According to National Archives CUI Registry (CUI Registry), CTI has the following characteristics:
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.
"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" (U.S. Government Publishing Office: Electronic Code of Federal Regulations).
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.
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" (DTIC: Distribution Statements & Their Corresponding Reasons for Use)
The term does not include information that is lawfully publicly available without restrictions.

Figure 4: Definition of Controlled Technical Information

Not all data on a DoD contractor unclassified networks would be classified as CTI. Some examples include financial data, human resource data, internal governance, sales data, holiday party pictures, co-mingled personal use data, and so forth. In fact, less than 10% of all data at rest in a DoD unclassified network would be considered controlled technical information. The challenge for most contractors will be to identify their CTI, which is essentially all technical information relevant to the design, development and manufacturing of DoD contract products because CTI and non-CTI are co-mingled in email, on file shares and in data bases.

The DFARS 252.204-7012 Clause

The Defense Federal Acquisition Regulation Supplement (DFARS) is a part of the Defense Procurement and Acquisition Policy (DPAP). The DFARS is the Department of Defense (DoD) extension to the Federal Acquisition Regulation (FAR). “The DFARS contains requirements of law, DoD-wide policies, delegations of FAR authorities, deviations from FAR requirements, and policies/procedures that have significant impact to the public.” [17] To put it simply, DFARS is the method that the DoD uses to procure products and services from DoD contractors.

On November 18, 2013, an initial ruling requiring released requiring minimum security controls for safeguarding controlled technical information on DoD contractor unclassified information systems was published in DFARS clause 252.204-7012. [22] This initial ruling had three parts as follows:

1. **Incident Reporting**: DoD contractors must report cyber security incidents involving the exfiltration of CUI to the DoD CIO within 72 hours of discovery.
2. **NIST SP 800-53 Partial Compliance:** The DoD contractor must be in compliance with a subset of controls the National Institute of Standards and Technology special publication 800-53 (aka NIST SP 800-53). [13]
3. **Compliance in DoD Contractor Supply Chain:** DoD contractors are required to flow down 252.204-7012 requirements to subcontractors who store, process or generate Controlled Technical Information as part of contract performance.

On December 30th, 2015, the final ruling of the DFARS clause was issued. [23] The revised clause referred to a new NIST special publication 800-171. NIST SP 800-171 included 109 controlled technical information safeguarding controls. DoD contractors would have to be 100% compliant with NIST SP 800-171. [24] The final ruling gave DoD contractors until December 31st, 2017 to meet compliance.

On December 6th, 2016, NIST SP 800-171 revision 1 was published. NIST SP 800-171r1 included one significant enhancement called the System Security Plan (SSP), to bring the total control count to 110. More on the SSP in the next section.

Details of the Clause

Part 1: Incident Reporting

A contractor must report an incident involving an exfiltration of controlled technical information within 72 hours of discovery to both 1) the prime contractor if applicable and in parallel to 2) the DoD at the following DFAR directed site: DOD Dibnet (dibnet.dod.mil).

An interesting twist to keep in mind is that the average detection time of a cyber breach, per FireEye, is 146 days. [23] Further, more than 60% of the time, companies are made aware of breaches by an external party, often the FBI. When this is the case, it’s difficult for a contractor to have comprehended the full extent and cause of a cyber breach within 72 hours of discovery.

The DoD contractor can leverage advanced detection service like those provided by Dell SecureWorks [24], using their endpoint threat detection and their Counter Threat Unit. The combination of threat detection technology and a group of knowledgeable analysts are critical to early detection and incident response.

Advanced incident detection services are expensive, and may be beyond the price range of the majority of our 33,000 defense contractors. But there isn't anything in the clause that requires a minimum timeframe between breach and detection. The requirement is to report within 72 hours from the time of detection. Thus, the Incident Reporting part of the DFARS 252.204-7012 is relatively easy to fulfill.

Part 2: NIST SP 800-171 Safeguarding Controls

The NIST SP 800-171r1 standard contains 110 safeguarding controls that are mainly concerned with maintaining the confidentiality of controlled unclassified information. The standard is titled "Protection Controlled Unclassified Information in Nonfederal Organizations."

The standard aligns with "the Federal Information Security Modernization Act (FISMA), which requires federal agencies to identify and provide information security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of (i) information collected or maintained by or on behalf of an agency; or (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." [27] FISMA is comprised of many publications, including the Federal Information Processing Standard FIPS-200, "Minimum Security Requirements for Federal Information Systems," and NIST 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations." NIST SP 800-171 are derived specifically from FIPS 200 and are a subset of NIST 800-53. [28] [13]

NIST SP 800-171 contains only three chapters: 1) Introduction, 2) The Fundamentals, and 3) The Requirements, a.k.a, "The 110 Controls." Chapter 1: is essentially the who, what, where, when and why of NIST SP 800-171. It explains the need to protect CUI, the motivation of the Executive Order 13556, the deficiencies that are addressed by the CUI program, the purpose and applicability and the target audience. Chapter 2: Describes the assumptions and methodology for developing requirement for safeguarding controlled technical information. Chapter 2 describes how the controls in Chapter 3 are categorized by type (basic and derived) and family (control groups). The control families are taken directly from FIPS-200. The basic and derived controls are taken directly from NIST SP 800-53. Mappings from NIST SP 800-171 to NIST SP 800-53 are provided in Appendix D of NIST SP 800-171.

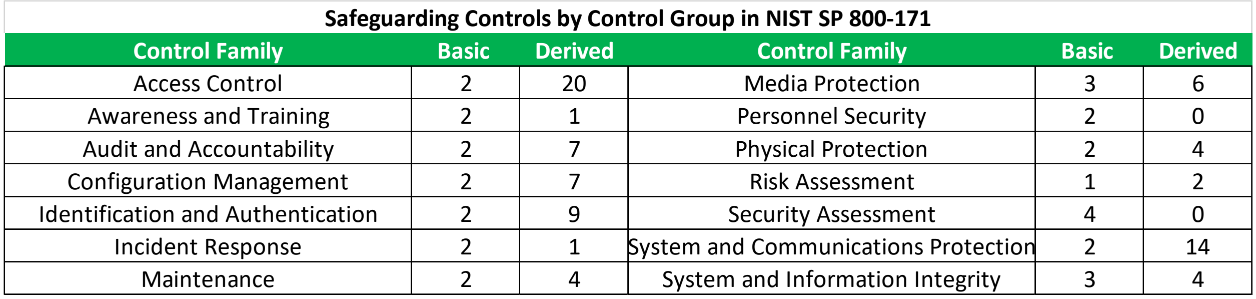
Basic controls establish and enforces the following where CTI is stored or processed:

- Establishing and maintain baselines and inventories throughout system lifecycles
- Enforcing baselines in all relevant systems (where CTI is stored or processed)

Derived controls ensure the following where CTI is stored or processed:

- Ensure change management controls
- Ensure that changes for security impact are analyzed before changes are made
- Ensure physical and logical access restrictions associated with changes
- Employ the principle of least functionality in configuration and changes
- Ensure restriction of nonessential programs, functions, ports, protocols and services
- Ensure deliberate control of approved software and ensures blacklisting of unauthorized software
- Ensure the monitoring and control of user installed software

Basic and Derived controls are applied to the fourteen FIPS-200 control families. There are 30 basic controls and 79 derived controls comprising the 110 controls.



Safeguarding Controls by Control Group in NIST SP 800-171

Control Family	Basic	Derived	Control Family	Basic	Derived
Access Control	2	20	Media Protection	3	6
Awareness and Training	2	1	Personnel Security	2	0
Audit and Accountability	2	7	Physical Protection	2	4
Configuration Management	2	7	Risk Assessment	1	2
Identification and Authentication	2	9	Security Assessment	4	0
Incident Response	2	1	System and Communications Protection	2	14
Maintenance	2	4	System and Information Integrity	3	4

Figure 5: Safeguarding Controls by Control Group and Type

The 110th control is the System Security Plan (SSP). As mentioned earlier in the report, the SSP was not a part of the original version of 800-171, but was added in Revision 1 published in December of 2016.

The ultimate purpose of the SSP is to demonstrate to relevant federal agencies and prime contractors the implementation or planned implementation of the security requirements of DFARS 252.204.7012 in NIST SP 800-171. As stated in NIST SP 800-171:

> "Federal agencies may consider the submitted system security plans and plans of action as critical inputs to an overall risk management decision to process, store, or transmit CUI on a system hosted by a nonfederal organization and whether or not it is advisable to pursue an agreement or contract with the non-federal organization." [22]

To translate "the ultimate purpose" above in a different way, "planned implementation of security requirements" means that 100% of the safeguarding controls are not required to be in place before December 31st, 2017 as long as the contractor has a plan of action to become compliant and the contracting officer agrees with the SSP's mitigations. A contracting officer at the DoD or a prime contractor is empowered to accept a SSP as documentation of compliance, even if the DoD contractor doesn't comply with all 110 safeguarding controls.

It's important to note that some of the controls in 800-171 are expensive to implement. For example, control 3.13.8 requires that CTI be encrypted at rest. This can be a very costly to implement in the data center, where storage area networks are typically not encrypted at the drive level. However, companies tend to continually refresh and updating the IT infrastructures. An SSP can be leveraged to align IT infrastructure upgrade plans within the SSP plans of action.

The SSP can also be a strategic document for a DoD contractor to use as an IT risk management framework. DFARS compliance requirements and gaps can be communicated to contractor employees through the SSP, or by using the SSP as a baseline reference. The contractor accomplished two objectives 1) Enlisting the organization in the coordination of continuous improvement in risk posture and to closing compliance weaknesses, and 2) Reinforcing employee awareness, satisfying requirements in the "Awareness and Training" control family. The "NIST SP 800-171 System Security Plan" should be comprehensively updated annually, at a minimum, as part of compliance with DFARS 252.204-7012." A well written SSP, including a solid safeguarding controls strategy and reasonable plans of action to close compliance gaps is the key to DFARS compliance.

Part 3: Compliance Oversight of DoD Contractor Supply Chain

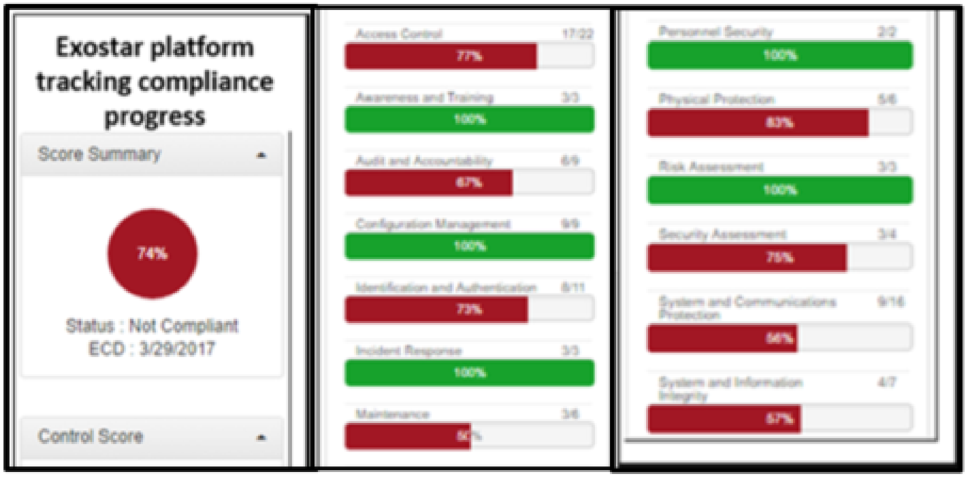
Within the DoD contractor ecosystem, there are prime contractors and subcontractors. Prime contractors are the DoD contractor who is awarded the contract from the DoD. Sub-contractors are contracted by prime contractors to facilitate contract delivery. For example, Northrop Grumman wins a contract to build an aircraft carrier, the subcontract thousands of subsystems to build the carrier, like the nuclear propulsion system, the electrical system, the aircraft control system, etc.

The third part of DFARS compliance requires that DoD contractors are also responsible for ensuring and monitoring the DFARS compliance of any subcontractor in their supply chain where CTI is exchanged as part of contact fulfillment. Unfortunately, this isn't an efficient way to thoroughly accomplish this part, and can only be accomplished through best effort. With a DoD ecosystem of more than 33,000 contractors, and each contractor a continually improving and evolving path towards DFARS compliance, ensuring and monitoring compliance is a monumental requirement.

This is further complicated by the fact that since the DoD did not include an auditing or certification mechanism as part of DFARS 252.204-7012 compliance. DoD contractors will not (at the time of this writing) have an independent third party assess compliance, and provide a certification that can be used to prove compliance to contracting officers.

> “No new oversight paradigm is created through this rule. If oversight related to these requirements is deemed necessary, then it can be accomplished through existing Federal Acquisition Regulation (FAR) and DFARS allowances, or an additional requirement can be added to the terms of the contract. The rule does not require “certification” of any kind. By signing the contract, the contractor agrees to comply with the contract's terms.” [29]

DFARS compliance relies on the DoD contractor’s self-attestation, and compliance is a moving target. To make this even harder, assessing a subcontractors System Security Plan (or cyber questionnaire in use now by some prime contractors) can only be interpreted by an experienced cyber security professional. Cyber security professionals are in limited supply in most DoD contractors, and they’re busy closing the gaps on their own company’s compliance situation.



Exostar platform tracking compliance progress

Score Summary ▲

74%

Status : Not Compliant
ECD : 3/29/2017

Control Score ▲

Access Control 17/22 77%

Awareness and Training 3/3 100%

Audit and Accountability 6/9 67%

Configuration Management 9/9 100%

Identification and Authentication 8/11 73%

Incident Response 3/3 100%

Maintenance 3/6 50%

Personnel Security 2/2 100%

Physical Protection 5/6 83%

Risk Assessment 3/3 100%

Security Assessment 3/4 75%

System and Communications Protection 9/16 56%

System and Information Integrity 4/7 57%

Figure 6: The Exostar Subcontractor Assessment Platform

As all DoD contractors are busy closing the gaps on compliance, their compliance assessments change, questionnaires need to be updated, and the assessors need to re-review.

There is also risk associated with contractors haphazardly assessing each other without a secure collaboration platform, since implementation of safeguarding controls, can provide vulnerability information to be exploited if they fell in the wrong hands. Vulnerabilities are only exploited wen they are discovered. Consequently, the exchange of assessment information increases the likelihood that a vulnerability will be discovered by a threat actor.

There is at least one company that provides a robust and secure platform for monitoring compliance of the supply chain. The company, called Exostar [25], allows DoD contractors to complete a DFARS cyber security questionnaire one time, and then connect the results of the questionnaire to prime contractors who are doing the oversight. The benefit to the DoD contractor is they can manage their compliance reporting in one place, as long as their prime contractors are using the platform (most of the major DoD prime contractors are). Then, for prime contractors, the Exostar platform allows contracting officer (or cyber professional) to view compliance reporting in an efficient manner.

Intended Outcome of the DFARS Clause

The DFARS clause has created a CTI safeguarding expectation within the DoD contractor community, and between DoD contractors and the DoD. Timely reporting of breaches of CTI can be disseminated to the DoD as well as to other DoD contractors, helping all to prepare for and to identify the unique indicators of compromise of the threat actors. While a significantly motivated threat actor is difficult to stop, safeguarding controls and information sharing will slow down a threat actor, and threat actor offensive operations will be more expensive. As NIST SP 800-171 bakes into all DoD contractor business operations, cyber security performance will continually improve.

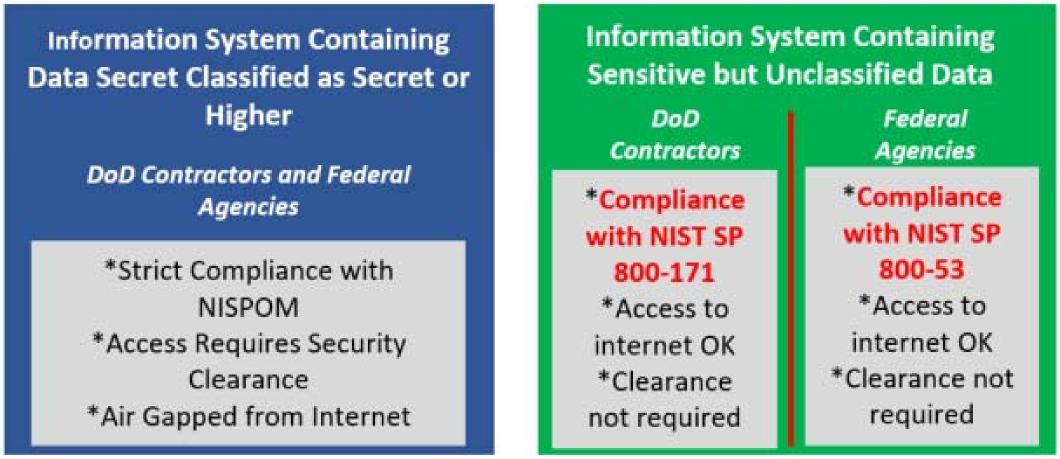

Information System Containing Data Secret Classified as Secret or Higher
DoD Contractors and Federal Agencies
*Strict Compliance with NISPOM
*Access Requires Security Clearance
*Air Gapped from Internet
Information System Containing Sensitive but Unclassified Data
DoD Contractors
Federal Agencies
*Compliance with NIST SP 800-171
*Access to internet OK
*Clearance not required
*Compliance with NIST SP 800-53
*Access to internet OK
*Clearance not required

Figure 7: Cyber Security in Military Industrial Complex After 12/31/2017

But the U.S. taxpayer/citizen is the greatest beneficiary to continually improving cyber security in the MIC. With continually improving cyber security, defense spending investments are better protected. The U.S. strategic defensive advantage will widen in proportion to the U.S. dominance in spending. Most importantly, the U.S. taxpayer/citizen will be more assured that national security is not weakened by poor cyber security in the MIC.

DoD Contractor Benefits

Although DoD contractors realize it is in their best interest to have a robust information assurance program, they have been limited in executing comprehensive cyber programs due to the supplemental costs and the competitive nature of winning contracts. But the new DFARS regulation levels the playing field where all contractors must now invest in the supplemental costs of implementing the controls in NIST SP 800-171.

The larger DoD contractors have historically had more at stake against cyber threats. Big high-profile contractors like Lockheed Martin and Boeing are have mature cyber programs, as the DoD has held them to individual standards as part of winning multi-billion dollar contracts.

However, the bottom 99% of DoD contractors have had little financial incentive to apply robust cyber security programs in their companies. Cyber security cost money and impacts business operations. Smaller DoD contractors must be very competitive to win contracts. With the DFARS clause, DoD contractors have a new differentiator to leverage a strategic advantage. DoD contractors who can efficiently execute DFARS compliance will leverage a strategic advantage.

Unintended Outcome of the DFARS Clause

As of the time of this writing, most of the 33,000 companies who sell to the DoD have little grasp for how DFARS 252.204-7012 connects to NIST SP 800-171, and how that is a subset of NIST SP 800-53, and how that is an outcome of FIPS-200, and how that is an outcome of FISMA, and that 800-171 is a response to Executive Order 13556 to ensure protection of controlled unclassified information, and that executive order assigned the National Archives as the administrative agency, who defines the properties of the controlled unclassified information that contractors are accountable to protect through the safeguards in 800-171. To be sure, DFARS compliance is complicated and highly technical. Most of the 33,000 companies selling to the DoD have fewer than 100 employees, and/or are companies whose main business is not DoD contracts, and consequently do not have staff expertise capable of managing DFARS compliance.

The DoD did not intend for the DFARS clause to create a new market opportunity to be exploited by private industry. The DoD foresaw that contractors would use the ramp up time to the DFARS compliance deadline to efficiently adopt the controls in NIST SP 800-171. But because of the DFARS challenge to contractors, private industry is swooping in with solutions to help become compliant and sustain compliance.

To watch the market evolve and grown for DFARS solutions providers, a Twitter hashtag search of #DFARS shows companies entering the DFARS solutions market every week. A few examples with summary offerings include the following:

Sera Brynn - "The New DFARS COMPLIANCE 252.204-7012 and you, the U.S. Government Contractor - We help your business achieve compliance through our DFARS Part 252.204-7012 Compliance and Assessment Services." [28]

Trustifier – DFARS Compliance-Kit – Make your business DFARS compliant by the 15th of May at a fraction of the cost of a DIY home-grown compliance solution. [29]

Coalfire – "DFARS/NIST 800-171 Simplifying Compliance through Automation - Join AWS and Coalfire for this free webinar on managing DFARS 252.204-7012 and NIST 800-171 compliance hosted on AWS, managed with Splunk and delivered by Coalfire" [30]

I2Act – "Reach Your Cyber Summit – All DoD Contractor and Subcontractors are required to be in compliance with DFARS 252.204-7012 by December 31st, 2017 and must complete a cyber assessment, present a remediation plan and status of compliance and provide a POA&M" [31]

And, as mentioned in "Part 3: Compliance Oversight in the DoD Supply Chain," the **Exostar** platform helps contractors manage DFARS compliance in the supply chain.

Risks to the DFARS Clause

As of December 31st, 2017, all 33,000 DoD contractors are expected to be in compliance with DFARS 252.204-7012 if the clause was written into a contract the contractor was awarded. If the contractor was awarded the contract as early as 2015, it's likely the clause was in the contract. But the DoD has no mechanism in place for measuring evolving state of compliance for DoD contractors. Many DoD contractors are accepting awarded contracts with the clause, and choosing to worry about compliance later. Further, as discussed earlier, the compliance process does not include a certified third party audit. Instead the compliance process relies on the honor system, which is called "self-attestation." The DoD will not know for certain whether DoD contractors are running robust compliance programs. Gaps in a contractor's compliance program will be revealed if and when the contractor reports a breach of CUI/CTI, and if the breach is bad enough to warrant an investigation. With DFARS compliance complexity, scope, costs, behavioral changes, and lack of expertise, the conditions for significant industry-wide compliance gaps are high.

Specific Risk to the DoD

The DoD will become increasingly aware of industry-wide compliance gaps in the weeks and months following the compliance deadline. Thus, there will be a gradual realization that the overwhelming numbers of links in the supply chain are non-compliant. The DoD will not be able to shut down the supply chain, yet the law requires compliance with the DFARS clause. How the DoD will navigate through this likelihood is uncertain.

Specific Risk to the DoD Contractor

Aside from the fact that the contractor stands to lose DoD contracts for non-compliance, there is the penalty for misrepresenting DFARS compliance. The penalty for a breach of obligations is as follows: "(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." [32]

Compliance Strategies

The DoD Defense Industrial Base partnership [33] categorizes DoD contractors as small, medium and large. The categorization provides a simple reference to the number of employees working for the defense contractor, since the number of employees is a reasonable indicator of the contractor's IT and Cyber capability. Large contractors have greater than 10,000 employees, medium contractors have between 1000-10,000 employees, and small contractors have less than 1000 employees.

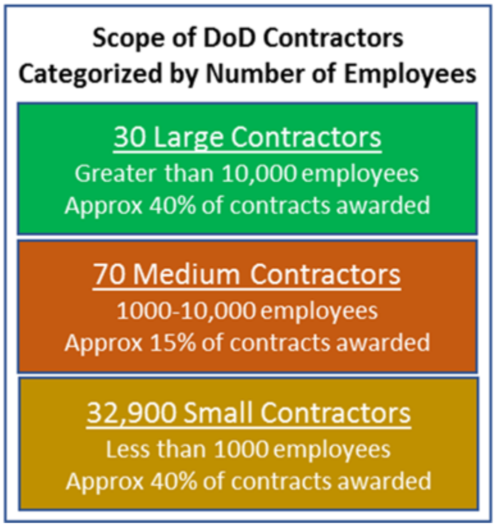

Scope of DoD Contractors
Categorized by Number of Employees
30 Large Contractors
Greater than 10,000 employees
Approx 40% of contracts awarded
70 Medium Contractors
1000-10,000 employees
Approx 15% of contracts awarded
32,900 Small Contractors
Less than 1000 employees
Approx 40% of contracts awarded

Figure 8: Scope of DoD Contractors Categorized by Number of Employees

Of the $300 billion in defense contracts awarded in 2015, $135 billion were awarded to large defense contractors, comprising the top 30, with medium sized contractors comprising 31 – 100, totaling $40 billion more in contracts. [5] With the total scope of DoD contractors in 2015 estimated to be 33,000, the remaining $125 billion in contracts were awarded to 32,900 contractors. It's impossible to be exacting in identifying the dividing line is between large, medium and small, since DoD contracts awards are not proportional to the number of employees in companies. The size of contract award is simply being used as a barometer to identify number scope of the number of companies in each category, and the compliance strategy they can consider using. The graphic at right shows a reasonable estimate for number of DoD contractors in each category.

Small DoD Contractor Compliance Strategy

Small contractors often lack the technical or compliance staff needed to comprehend the safeguarding requirements in DFARS. In addition, small contractors are typically subcontractors to the medium and large contractors (bigger contractors), although they also win contracts directly from DoD. The pressure to comply to DFARS will be from the large and medium contractors.

However, that pressure is a long way from critical mass. The bigger contractors are still focusing on their own compliance gaps. It will take a year or two from the compliance deadline of December 31st, 2017 for the bigger contractors to mature their DFARS compliance efficiencies such that they can enhance focus on the small contractors. In the meantime, the majority of small contractors are largely unaware or are underestimating the safeguarding compliance at hand.

Yet, as time progresses, the industries "tribal knowledge" will evolve in developing smart and efficient compliance strategies that can be applied in a small contractor environment. The tribal knowledge available now is already being productized and sold by companies like the ones mentioned in "Unintended Outcome" section above.

In terms of DFARS compliance, the advantage for small DoD contractors is that they typically have information infrastructures that are far less complex than the bigger contractors. Remember that DFARS only requires safeguarding of controlled technical information (CUI/CTI). A smaller contractor can more easily isolate their CTI to a small group of computers within their infrastructure, and define this as the security boundary where safeguarding controls are applied. Working with a smaller information infrastructure, and a finite data footprint, a subject matter expert could shorten the NIST SP 800-171 learning curve and help a small company to compliance within days or weeks, depending on the starting point compliance gap.

Medium DoD Contractor Compliance Strategy

Medium contractors have the greatest challenge in terms of DFARS compliance. There are several characteristics about medium contractors that, taken together, make DFARS particularly challenging.

- Information assurance programs that are less mature than large contractors.
- Diverse information infrastructures that can span across the US (sometimes international).
- Organically grown information infrastructures (often through mergers and acquisitions) that are weak in central governance

- Data sprawl across the information infrastructure, making CUI/CTI difficult to identify and manage.
- Boundaries of acceptable use corporate culture leans towards permissive and risky.
- Executive leadership focus to minimize overhead costs, prioritizes IT capability over IT risk reductions

These characteristics are always applicable, but obviously in varying degrees. Medium contractors often compete with large contractors or with other medium contractors, and price being the main differentiator. Keeping costs down, especially overhead costs, allows medium contractors to win and grow. This is why medium contractors have less mature information assurance programs than larger contractors, who can spread overhead costs among thousands more employees. Thus, the typical medium contractor has bigger compliance gaps to close than the typical large contractor.

By now, every medium contractor has identified the staff member accountable to DFARS compliance. The Chief Information Security Officer (CISO) is where accountability falls by default according to FISMA. But many medium contractors have yet to fill the CISO role, in which case the accountability will be assigned to the CIO or the organizational lead for government compliance. Whoever the accountable person is, its highly likely they have not figured out how to close all the gaps before the compliance deadline.

The key to closing the compliance gap for medium contractors is the 800-171 System Security Plan (SSP), described in “Part 2: NIST SP 800-171 Safeguarding Controls.” A well written SSP, with reasonable plans of action for closing compliance gaps (even beyond the compliance deadline) provides the strategic framework for the medium contractor. Medium contractors should leverage the SSP as the strategic document that aligns expectations of the organization with the prime contractor of DoD.

Medium contractors facing the DFARS compliance challenge should also comprehend the unique advantages they have compared to large contractors. For example, a CISO (or the staff member accountable for DFARS compliance) driving compliance in a medium contractor organization can usually leverage a higher degree of agility than a large contractor. In addition, CISO's who've historically fought for priority of information security versus capability can leverage DFARS compliance to increase priority.

Large DoD Contractor Compliance Strategy

Large contractors are different from small and medium contractors because they already have mature information assurance programs. The cyber security spotlight has been on large DoD contractors at least since the Chinese hacked Lockheed Martin in 2009 and stole a huge amount of design and electronics data on the F-35. [17]

In lieu of the mandatory standard that is NIST SP 800-171, the DoD has been pushing the larger contractors articulate information assurance programs as part of the winning the largest contracts. The DoD has used NIST SP 800-53 as the benchmark to compare information assurance programs large contractors. Thus, the mature information assurance programs in place at the large contractors are based on 800-53, which is the super set of safeguarding controls in 800-171.

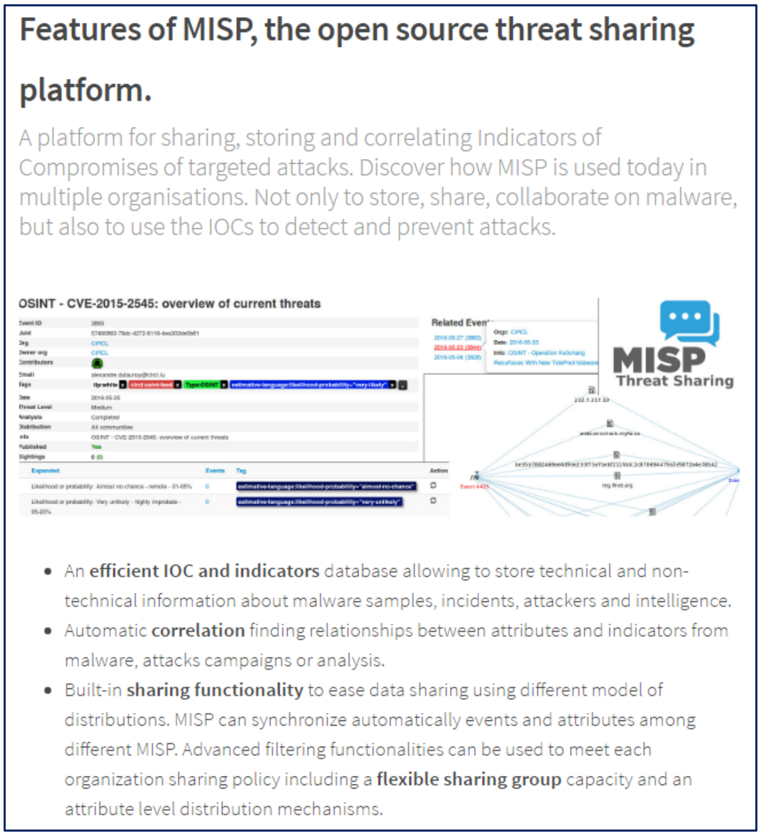
Nevertheless, this does not mean the large contractors are 100% compliant with 800-171. It simply means that their compliance gaps are much smaller. Instead of wrestling with compliance of 60% of the 109 safeguarding controls as a small contractor would be, or 30% of the safeguarding controls as a medium contractor would be, the large contractor is wrestling with compliance on less than 5% of the safeguarding controls of 800-171. In almost all cases, the large contractor is struggling with multi-factor authentication safeguards, encryption at rest safeguards, and encryption in transit safeguards. In all cases, these safeguards have been applied to parts of their information infrastructure, but not yet reaching 100%.

The compliance strategy for the large contractor is simple: Write an SSP that describes the plan of action for closing the gaps on the specific safeguarding controls.

The Future of DoD Cybersecurity Compliance

On February 12, 2015, President Obama signed Executive Order 13691 promoting cyber security information sharing between and among private industry and the government. [34] From a DFARS compliance standpoint, this is somewhat an extension of the part requiring incident reporting within 72 hours of incident detection. DFARS compliance is a critical milestone for all DoD contractors, especially the medium and small contractors who will develop information assurance programs as an outcome. But the 109 safeguarding controls that comprise 800-171 are obstructions to threat actors, they won't stop the threat actors from being successful. "Great Wall defenses could be leapt over or maneuvered around. Instead, cyber security teams, civilian and military, should focus on detection and resilience – designing systems that could spot an attack early on and repair the damage swiftly." [12] Information sharing is the key to detection, and automation is the key sharing information quickly.

The Defense Security Information Exchange is a non-profit organization formed with a mission of sharing information about threat actors within the DoD contractor community. [35] Since the nation-state threat actor groups who target DoD contractors use the same tactics, techniques and procedures (TTPs) and indicators of compromise (IOCs) no matter who they are hacking, the DSIE was formed to share the TTPs and IOCs amongst the community. This collaboration is extremely effective in improving detection and improving countermeasures against the worlds most skilled hackers.



Features of MISP, the open source threat sharing platform.

A platform for sharing, storing and correlating Indicators of Compromises of targeted attacks. Discover how MISP is used today in multiple organisations. Not only to store, share, collaborate on malware, but also to use the IOCs to detect and prevent attacks.

- An **efficient IOC and indicators** database allowing to store technical and non-technical information about malware samples, incidents, attackers and intelligence.
- Automatic **correlation** finding relationships between attributes and indicators from malware, attacks campaigns or analysis.
- Built-in **sharing functionality** to ease data sharing using different model of distributions. MISP can synchronize automatically events and attributes among different MISP. Advanced filtering functionalities can be used to meet each organization sharing policy including a **flexible sharing group** capacity and an attribute level distribution mechanisms.

Figure 9: Contractor Threat Information Sharing of the Near Future

The next level of sophistication for DoD contractors to improve detection and resilience is to automate where possible. There are many platforms available to achieve TTP and IOC automation, for example the Malware Information Sharing Platform (MISP). [36]

DoD contractor information sharing collaboration is a powerful countermeasure against nation-state threat actors. The earlier TTPs and IOCs are identified, the costlier offensive operations become, with each attack requiring a new strategy. However, there are some in the

DoD contractor community who think that information sharing is a two-way street, meaning that they are willing to share TTPs and IOCs to other contractors who will also provide reciprocal TTPs and IOCs. This is not surprising considering DoD contractors are often competing for contracts, so why give valuable information away to a potential competitor. Others see the information sharing among DoD contactors as an issue of national security, so let the contractors compete for contracts, but the cyber community should work together regardless.

Executive Order 13631 recognizes that information sharing is in the best interest of the United States. This is already being proven within the DoD contractor community through the DSIE. Information sharing trends will continue to improve. At some point in coming years, DFARS clause will evolve to add information sharing as a part of compliance.

Conclusion

The U.S. Federal Government spends more than 50% of the discretionary budget on defense, and 75% of the military budget is spent with DoD contractors. On December 31st, 2017, DoD contractors will, for the first time, be required by law to protect controlled technical information in their unclassified networks. Controlled technical information has been targeted and exfiltrated by nation state threat actors for several years, for the purpose of replicating U.S. defensive capabilities. Nation-state threat actors will continue to steal U.S. technology, so DoD contractors must be held to minimum safeguarding standards. The For as much as the U.S. prioritizes in defense spending, the American taxpayer should expect that we adequately protect the U.S military intellectual property from espionage. It is the duty, and now the law, for all DoD contractors meet and exceed the DFARS clause.

References

[1] "Military-industrial complex," Wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/Military%E2%80%93industrial_complex. [Accessed 21 February 2017].

[2] "National Security Decision Directive 145," IT Law Wiki, [Online]. Available: http://itlaw.wikia.com/wiki/National_Security_Decision_Directive_145. [Accessed 2 May 2017].

[3] D. R. G. G. Rick Lehtinen, in *Computer Security Basics*, Sebastopol, CA, O'Reilly Media, 2006, 1991, p. 296.

[4] D. Sanger, "RISE AND FALL OF U.S. DATA DIRECTIVE," *New York Times,* 19 March 1987.

[5] "Mandatory Spending," Wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/Mandatory_spending. [Accessed 25 April 2017].

[6] "Stockholm International Peace Research Institute," [Online]. Available: http://books.sipri.org/files/FS/SIPRIFS1604.pdf. [Accessed 21 February 2017].

[7] "Top-100 Defense Contractors 2015," Aeroweb, [Online]. Available: http://www.fi-aeroweb.com/Top-100-Defense-Contractors-2015.html. [Accessed 27 February 2017].

[8] "FY 2015 DOD Contractors with Awards of $25,000.00 or more," Office of the Army General Counsel, [Online]. Available: http://ogc.hqda.pentagon.mil/EandF/Documentation/contractor_list.pdf. [Accessed 23 February 2017].

[9] M. Kassner, "Anatomy of the Target data breach: Missed opportunities and lessons learned," ZDNet, 2 February 2015. [Online]. Available: http://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/. [Accessed 26 April 2017].

[10] "National Archives EO 12829," [Online]. Available: https://www.archives.gov/isoo/policy-documents/eo-12829.html. [Accessed 02 03 2017].

[11] "Wikipedia National Industrial Security Program," [Online]. Available: https://en.wikipedia.org/wiki/National_Industrial_Security_Program. [Accessed 2 March 2017].

[12] "Chapter 8: Information System Security," in *National Industrial Security Program Operating Manual*, Arlington, Virginia, National Industrial Security Program, 2006, p. 141.

[13] J. L. Grama, Legal Issues in Information Security, Burlington, MA: Jones and Bartlett Learning, 2015.

[14] "NIST SP 800-53 rev 4," National Institute of Standards and Technology, April 2013. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. [Accessed December 2016].

[15] R. A. Clarke, "Chapter 2: Cyber Warriors," in *Cyber War*, New York, Harper Collins, 2010, p. 306.

[16] "Statistics.com," [Online]. Available: http://statisticstimes.com/economy/countries-by-projected-gdp.php. [Accessed 25 March 2017].

[17] T. C. a. T. Atlas, "Bloomberg," 8 May 2015. [Online]. Available: https://www.bloomberg.com/news/articles/2015-05-08/china-advances-threaten-erosion-of-u-s-advantage-pentagon-says. [Accessed 20 March 2017].

[18] "F-35 Lightning II," Lickheed Martin, [Online]. Available: https://www.f35.com/about/history. [Accessed 6 March 2017].

[19] M. Mount, "Hackers stole data on Pentagon's newest fighter jet," CNN.com, 21 April 2009. [Online]. Available: http://www.cnn.com/2009/US/04/21/pentagon.hacked/. [Accessed 22 April 2017].

[20] "Theft of F-35 design data is helping U.S. adversaries -Pentagon," Reuters, [Online]. Available: http://www.reuters.com/article/usa-fighter-hacking-idUSL2N0EV0T320130619. [Accessed 6 March 2017].

[21] "Code of Federal Regulations," Government Purchasing Office, [Online]. Available: https://www.gpo.gov/fdsys/pkg/CFR-2006-title32-vol6/xml/CFR-2006-title32-vol6-part2002.xml. [Accessed 20 January 2017].

[22] "SUBPART 201.3--AGENCY ACQUISITION REGULATIONS," Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, [Online]. Available: http://www.acq.osd.mil/dpap/dars/dfars/html/r20081020/201_3.htm. [Accessed 3 February 2017].

[23] "Federal Register Vol. 78 No. 222," U.S. Government Publishing Office, 18 November 2013. [Online]. Available: https://www.gpo.gov/fdsys/pkg/FR-2013-11-18/pdf/2013-27313.pdf. [Accessed December 2016].

[24] "Defense Aquisition Regulation System 252.204–7012 Safeguarding Covered Defense Information and Cyber Incident Reporting," Government Purchasing Office, 30 December 2015. [Online]. Available: https://www.gpo.gov/fdsys/pkg/FR-2015-12-30/pdf/2015-32869.pdf. [Accessed December 2016].

[25] "NIST Special Publication 800-171," Natinional Institute of Standards and Technology, December 2016. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf. [Accessed December 2016].

[26] M. Lennon, "Breach Detection Time Improves, Destructive Attacks Rise: FireEye," Security Week, 25 February 2016. [Online]. Available: http://www.securityweek.com/breach-detection-time-improves-destructive-attacks-rise-fireeye. [Accessed February 2016].

[27] "Cyber Security: CTU Threat Intelligence Services," Dell Secure Works, [Online]. Available: https://www.secureworks.com/resources/vd-cyber-security-ctu-threat-intelligence-services. [Accessed February 2017].

[28] "DFARS," Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, [Online]. Available: http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012. [Accessed 10 12 2016].

[29] "Minimum Security Requirements for Federal Information and Information Systems," National Institite of Standards and Technology, March 2006. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf.

[30] "Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018)," Federal Register, 21 October 2016. [Online]. Available: https://www.federalregister.gov/documents/2016/10/21/2016-25315/defense-federal-acquisition-regulation-supplement-network-penetration-reporting-and-contracting-for.

[31] "Exostar Aerospace and Defense," Exostar, [Online]. Available: https://www.exostar.com/industry/aerospace-defense/. [Accessed 4 April 2017].

[32] "DFARS 7012 Safeguarding and Cyber Incident Reporting," Sera Brynn, [Online]. Available: https://sera-brynn.com/dfars/. [Accessed 4 April 2017].

[33] "Trustifier DFARS Compliance Kit," Trustifier.com, [Online]. Available: https://trustifier.com/?utm_source=Twitter%20&utm_medium=Tweet&utm_campaign=Infosec_Tourist. [Accessed 5 April 2017].

[34] "Coalfire DFARS/NIST 800-171," Coalfire.com, [Online]. Available: http://www2.coalfire.com/DFARS-NIST-800-171. [Accessed 5 April 2017].

[35] i2 Compliance Tools, [Online]. Available: http://www.i2compliancetools.com/. [Accessed 5 April 2017].

[36] "About the DIB CS Program," Defense Industrial Base Unclassified Network, [Online]. Available: https://dibnet.dod.mil/portal/intranet/Splashpage/RegisterThemed. [Accessed 21 January 2017].

[37] "Executive Order--Promoting Private Sector Cyber Security Information Sharing," The White House, [Online]. Available: https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari. [Accessed 21 January 2017].

[38] F. Kaplan, Dark Territory, New York, NY: Simon & Shuster, 2016.

[39] "Defense Security Information Exchange," DSIE, [Online]. Available: https://dsie.nc4mc.com/web/guest/home?p_p_id=58&p_p_lifecycle=0&_58_redirect=%2F. [Accessed 21 January 2017].

[40] Malware Information Sharing Platform, [Online]. Available: http://www.misp-project.org/features.html. [Accessed 6 February 2017].

[41] "Natinional Priorities Organization," [Online]. Available: https://www.nationalpriorities.org/budget-basics/federal-budget-101/spending/. [Accessed 28 February 2017].

[42] "Business Insider," [Online]. Available: http://www.businessinsider.com/how-the-us-military-spends-its-billions-2015-8. [Accessed 23 February 2017].

[43] "Defense Advanced Research Projects Agency," [Online]. Available: http://www.darpa.mil/about-us/about-darpa. [Accessed 2 March 2017].

[44] "Memorandum For The Heads Of Executive Departments And Agencies," The White House, [Online]. Available: https://georgewbush-whitehouse.archives.gov/news/releases/2008/05/20080509-6.html. [Accessed 23 March 2017].

[45] "Controlled Unclassified Information," National Archives, [Online]. Available: https://www.archives.gov/cui/about. [Accessed 2 February 2017].

[46] "Marking Controlled Unclassified Information," National Archives and Records Administration, 6 December 2016. [Online]. Available: https://www.archives.gov/files/cui/20161206-cui-marking-handbook-v1-1.pdf.