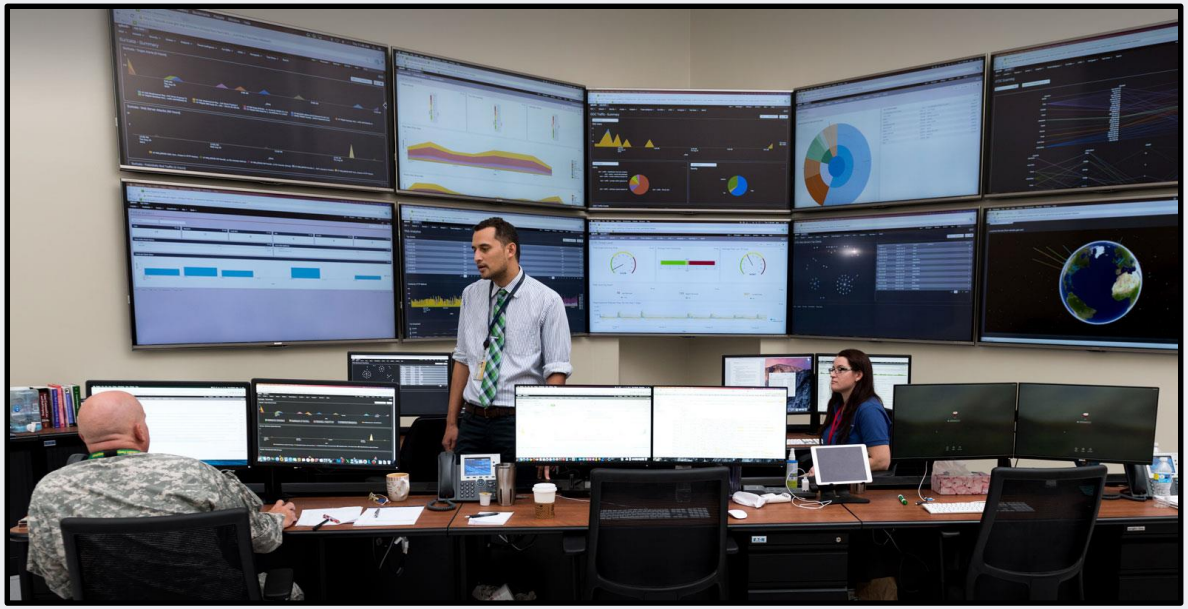
Complying with DoD Cybersecurity Requirements 101

Georgia Tech Enterprise Innovation Institute



By Andrew Smith

Jan. 14, 2019

My Contact Info

- Andrew E. Smith
- Procurement Counselor
- Georgia Tech Procurement

Assistance Center ("GTPAC")

- Andrew.Smith@innovate.gatech.edu
- Ph: 678-890-2342

Legal Disclaimer

- THIS PRESENTATION IS FOR INFORMATIONAL PURPOSES ONLY AND DOES NOT CONSTITUTE LEGAL ADVICE OR A LEGAL OPINION. THIS PRESENTATION IS NOT INTENDED TO CREATE, AND DOES NOT CREATE, AN ATTORNEY-CLIENT RELATIONSHIP BETWEEN THE PRESENTER AND THE PARTICIPANT.

Our To Do List

- The Threat and Current Cybersecurity Landscape
- What the Federal Government is Doing in Response
  - FAR 52.204-21
  - DoD: DFARS 252.204-7012 & NIST SP 800-171
- Contractor Compliance and Implementation
- Resources (Where to Get Help)
- Cyber Incident Reporting and Damage Assessment

Cybersecurity Threat and Landscape

- Crime and intelligence gathering is now commonly done in cyberspace.
- Cyber attackers utilize computer viruses, worms, trojan horses, ransomware, denial of service attacks, and other methods to break into, shutdown and/or sabotage computer systems.
- Cyber attackers often commit cyber theft, by stealing money and other things of value, such as intellectual property or one's identity. Cyber theft also includes embezzlement, fraud, and theft of personal or financial data.
- Cyber attackers now often sell information they steal on hidden portions of the Internet called the "dark web," which are typically virtual peer-to-peer networks that are only accessible to those with specific software, configurations or authorization.

Cybersecurity Threat and Landscape

Georgia Tech Enterprise Innovation Institute

Who does this stuff?

- It runs the gamut from computer geeks looking for bragging rights, to hacktivists looking to promote a political agenda, to organized crime syndicates looking to steal valuable information, to terrorists looking to shutdown critical infrastructure, to nation states who fund advanced operations to spy and rob the United States of its vital information.
- Today, the threat is much more serious than ever. Within the last 10 years, we've seen the rise of highly sophisticated, well-organized and funded cyberattacks. Many from state-sponsored groups.
- Most nation states now have advantage cyber warfare and espionage/intelligence apparatuses and capabilities (including China, North Korea, Iran, Russia).

Malware propagation

- Email is still the main vector for malware propagation.
- Analysis of major malware spam campaigns during 2016 found that "Invoice" was the most commonly used keyword in malware subject lines, other terms such as "Order," "Payment" and "Bill" were in the top 10.
- At GTPAC we've seen a huge increase in scammers mimicking the government – even using spoofed or stolen government email addresses.

2017 Symantec Internet Security Threat Report:
https://www.symantec.com/security-center/threat-report

OPM Breach

- In June 2015, the United States Office of Personnel Management (OPM) announced major data breach.
- 21.5 million identities of current and former government personnel were stolen, including Social Security numbers, and detailed security clearance related background information.
- Among the largest breach of government data in U.S. history.

F-35 Breach

- F-35 is The Joint Strike Fighter, a stealth multirole fighter that supports the US Navy, Air Force and Marine Corps.
- Using phishing emails and other tactics, a Chinese spy named Su Bin stole 630,000 files related to the F-35, totaling some 65 gigabytes of data.

PHOTOGRAPH OF SU BIN

F-35 Breach

Cybersecurity Threat and Landscape

- Government agencies continue to be targeted by a broad swathe of adversaries.
- Because of their proximity and close relationship with the government, government contractors are also attractive target for stealing intellectual property and information regarding government products, services, and operations worked on by the contractor.
- Attackers sometimes go after contractors and then try to "swim upstream" to the target agency.
- Attacks may be motivated by espionage or to disrupt government services or to expose or steal sensitive government related information.

What the Federal Government is Doing in Response

- In recent years there has been a strong push in the federal government to promulgate regulatory reforms to ensure that government contractors are implementing measures to safeguard their information systems.

FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems (JUN 2016)

- Identifies 15 security requirements for "basic safeguarding…covered contractor information systems."
- Covered contractor information system means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.
- Federal contract information means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public Web sites) or simple transactional information, such as necessary to process payments.

FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems (JUN 2016)

- Mandatory flow down to all non-COTS items
- Sets baseline of "minimum security controls" all government contractors must have.
- The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls…. (next 3 slides)

FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems (JUN 2016)

Georgia Tech Enterprise Innovation Institute

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

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

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

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

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

FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems (JUN 2016)

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

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

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

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

(10) 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.

FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems (JUN 2016)

Georgia Tech Enterprise Innovation Institute

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

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

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

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

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

- While these are the minimum requirements, Federal agencies and departments may prescribe additional safeguarding requirements relating to "covered contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information (CUI) as established by Executive Order 13556."

DoD Contractors

- All DoD solicitations and contracts (excepts COTs) are incorporating **DFARS 252.204-7012**, Safeguarding Covered Defense Information and Cyber Incident Reporting.

DFARS 252.204-7012

- DFARS Clause 252.204-7012 requires contractors/subcontractors to:
  - 1. Provide "adequate security" to safeguard "covered defense information" that resides on or is transiting through a contractor's internal information system or network.
  - 2. Report cyber incidents that affect a covered contractor information system or the covered defense information residing therein, or that affect the contractor's ability to perform requirements designated as operationally critical support.
  - 3. Submit malicious software discovered and isolated in connection with a reported cyber incident to the DoD Cyber Crime Center.
  - 4. If requested, submit media and additional information to support damage assessment.
  - 5. Flow down the clause in subcontracts for operationally critical support, or for which subcontract performance will involve covered defense information.

Purpose of DFARS 252.204-7012

- DFARS clause 252.204-7012 was structured to ensure that controlled unclassified DOD information residing on a contractor's internal information system is safeguarded from cyber incidents, and that any consequences associated with the loss of this information are assessed and minimized via the cyber incident reporting and damage assessment processes.
- In addition, by providing a single DOD-wide approach to safeguarding covered contractor information systems, the clause prevents the proliferation and safeguarding of controlled unclassified information clauses and contract language by the various entities across DOD.

Covered Defense Information

- What is CDI?
- A term used to identify information that requires protection under DFARS Clause 252.204-7012.
- CDI means:
  - Unclassified **controlled technical information (CTI)** or other information as described in the **CUI Registry** that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government wide policies and is –
  - (1) Marked or otherwise identified in the contract, task order, or delivery order and provided to contractor by or on behalf of, DoD in support of the performance of the contract; **OR**
  - (2) Collected, developed, received, transmitted, used, or stored by, or on behalf of, the contractor in support of the performance of the contract*

* "In support of the performance of the contract" is not meant to include the contractor's internal information (e.g., human resource or financial) that is incidental to contract performance

What is CTI?

- Controlled Technical Information
  - Technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.
  - To be marked with one of the distribution statements B through F, in accordance with DoD Instruction 5230.24, "Distribution Statements of Technical Documents."
  - Does not include information that is lawfully publicly available without restrictions.
  - E.g., 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.

CUI Registry

- Set up by the National Archives and Records Administration ("NARA")
- Online repository for information, guidance, policy, and requirements on handling Controlled Unclassified Information.
- Sets out procedures for the use of CUI, including but not limited to marking, safeguarding, transporting, disseminating, reusing and disposing of the information.

How do I know I have it?

- Existing DoD policy/regulations require DoD to:
- Identify covered defense information and mark information in accordance with DoD procedures for controlled unclassified information (CUI) found in DoDM 5200.01 Vol 4, DoD Information Security Program: CUI
- Document in the contract (e.g., Statement of Work, CDRLs) information, including covered defense information, that is required to be developed for performance of the contract,
  - Specify requirements for the contractor to mark, as appropriate, information to be delivered to DoD
- The contractor is responsible for:
  - Following the terms of the contract, which includes the requirements in the Statement of Work

How do I know I have it

- DoD Component or requiring activity is responsible for notifying the DoD Contracting Officer when a solicitation is expected to result in a contract that will require Controlled Unclassified Information to be (a) furnished by the Government and/or (b) developed or delivered by Contractors.
- When Controlled Unclassified Information is to be provided to or generated by DoD contractors, the controls and protective measures to be applied shall be described in the pertinent contract documents (e.g., contract clause; statement of work; or DD Form 254, "Department of Defense Contract Security Classification Specification"). **DoD Information Security Program: Controlled Unclassified Information (DoDM 5200.01, Volume 4, Feb 2012)**

I have it, now what?

- You must provide "**adequate security**" for the Covered Defense Information
- What does this mean? At a minimum, the contractor shall implement NIST SP 800-171, Protecting CUI in Nonfederal Information Systems and Organizations, **AND….**
- Apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to [NIST SP 800-171] may be required…

NIST SP 800-171

- It's a cybersecurity "standard" developed by the National Institute of Standards and Technology ("NIST")
- Provides standardized/uniform set of performance-based security requirements that must be implemented by DoD Contractors under DFARS 252.204-7012 to protect Covered Defense Information

Where do I get it?

- The publication is titled, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations," NIST SP 800-171 Revision 1, available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

NIST SP 800-171

- Most requirements in NIST SP 800-171 are about ensuring that the contractor has appropriate policy and process in place to protect its information systems, but meeting some requirements may require having certain security-related software or hardware.

NIST SP 800-171

- A reasonable approach to ensuring compliance:
  - Examine each of the requirements
  - Determine which requirements can be readily accomplished by in-house IT personnel by changing IT configurations of acquiring additional software and hardware, and which require additional research and assistance.
  - Develop plan of action and milestones to implement the requirements

DFARS Clause 252.204-7012

- By signing the contract, the contractor agrees to comply with the terms of the contract and all requirements of the DFARS Clause 252.204-7012.
- It is the contractor's responsibility to determine whether it is has implemented the NIST SP 800-171 (as well as any other security measures necessary to provide adequate security for covered defense information)
  - DoD will not certify that a contractor is compliant with the NIST SP 800-171 security requirements
  - Third party assessments or certifications of compliance are not required, authorized, or recognized by DoD.

System Security Plan and Plan of Action

- NIST SP 800-171 was revised (Revision 1) in December 2016, to require nonfederal organizations to demonstrate implementation with a "system security plan" and associated "plans of action."
- Security requirement 3.12.4 (System Security Plan) requires the contractor to develop, document, and periodically update, system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.
- Security Requirement 3.12.2 (Plans of Action) requires the contractor to develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in their systems.
- Organizations can document the system security plan and plan of action as separate or combined documents and in any chosen format.

What do I need to do to get compliant?

- You need to document implementation of NIST SP 800-171 immediately or you could risk losing your DoD contracts.
- Companies should have a system security plan in place, in addition to any associated plans of action to describe:
  - What NIST 800-171 Standards are met
  - How and when any unimplemented security requirements will be met
  - How any planned mitigations will be implemented
  - How and when they will correct deficiencies and reduce or eliminate vulnerabilities in the systems

3 Step Approach of Comply

- 1. Conduct a **Self-Assessment** against the SP 800-171 requirements, and produce a self-assessment report or checklist – This determines where you are, including the current effectiveness of the security employed.
- 2. Develop a **System Security Plan** that describes the (1) the system boundary; (2) the operational environment; (3) **how each of the security requirements are implemented**; and (4) the relationships with or connections to other systems.
- 3. Produce a **Plan of Action** that notes weaknesses and deficiencies and outlines appropriate response actions. This should outline how any unimplemented security requirements will be met and how any planned improvements will be implemented.

3 Step Approach to Comply

- We have provided resources to help you with this process: https://gtpac.org/cybersecurity-training-video/
- **Cybersecurity Self-Assessment Handbook** – The National Institute of Standards and Technology (NIST) Manufacturing Extension Partnership (MEP) Cybersecurity Self-Assessment Handbook was developed to assist U.S. manufacturers who supply products to the DoD implement NIST SP 800-171 as part of the process for ensuring compliance with DFARS Clause 252.204-7012. It should be noted that this Handbook can be utilized by any DoD contractor to help them conduct an assessment of their NIST SP 800-171 compliance.
- **Cybersecurity Template** – This is a 127-page template, developed by the Georgia Tech Procurement Assistance Center (GTPAC), designed to help contractors create a Security Assessment Report, System Security Plan, and Plan of Action. The template is a Word document, designed for easy customization. It is intended to be used in conjunction with the NIST-MEP Cybersecurity Self-Assessment Handbook linked above.

3 Step Approach to Comply

- NIST has provided a document, called NIST 800-171A that provides guidance to contractors on how to perform a proper assessment.
- Also, if you do not want to utilize our template, NIST has also developed and provided free templates to help you create the necessary System Security Plan and Plan of Action & Milestone documentation. See:
- https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final
- Be aware, that this 3 step process, while it sounds simple, can take a significant amount of time, depending on the sophistication of your information system. It could take two or three weeks of work – or longer to complete this process.

Other tools: CSET

- In the meantime, there is a tool you can use to help assess your IT security against NIST 800-171 called CSET you can download.
- No-cost application, developed by DHS's Industrial Control Systems Cyber Emergency Response Team, provides step-by-step process to evaluate controls.
- https://ics-cert.us-cert.gov/Assessments

Where can I get help?

- **Procurement Technical Assistance Centers** such as GTPAC can help: http://www.gtpac.org
- However, while we can tell you what steps you need to take, the assessment may need to be done by an IT professional.
- Determining compliance or what steps need to be taken to achieve IT compliance is highly dependent upon the IT system, its operating environment, the specific technologies available and whether and how they can be implemented based on your system and operating environment.

Where can I get help?

- There are also numerous IT consulting firms that have low-cost packages to help you with the assessment process and NIST 800-171 compliance.
- Probably best to use if you do not have adequate in-house IT staff or expertise.

Role of System Security Plan and Plans of Action

- NIST SP 800-171, Revision 1, Chapter 3: Federal agencies may consider the submitted system security plan 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 nonfederal organization.

Role of System Security Plan and Plans of Action

- How the plans may be utilized:
  - Solicitations may require proposals to include System Security Plans and identify any NIST SP 800-171 security requirements not implemented at the time of award and the associated plans of action for implementation.
  - Solicitations may indicate that the contractor's approach to providing adequate security will be evaluated in the source selection process.
  - E.g. if you don't get your system security compliant with 800-171, you will start to lose contracts involving CUI.

Subcontractor Flowdown

- DFARS clause 252.204-7012 flows down to subcontractors without alteration, except to identify the parties, when performance will involve operationally critical support or covered defense information.

Cloud Computing

- What happens under DFARS Clause 252.204-7012 if I use the cloud?
- Ensure the cloud service provider meets requirements equivalent to NIST 800-171, the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline.
- Still probably have to meet 800-171 on your in-house system because you are still *transmitting* CUI even if it is ultimately hosted in the cloud.

Cyber-Incident Reporting

- What is a cyber incident: An action(s) taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.
- Compromise means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.
- Must report cyber-incident within 72 hours. Reporting shall not, by itself, be interpreted as evidence that the contractor or subcontractor failed to provide adequate security.
- A cyber incident report via https://dibnet.dod.mil/

Cyber Incident Damage Assessment

- Government conduct cyber incident damage assessment.
  - Determine impact of compromised information on U.S. military capability underpinned by the technology;
  - Consider how the compromised information may enable an adversary to counter, defeat, or reverse engineer U.S. capabilities
  - Focus on the compromised intellectual property impacted by the cyber incident – not on the compromise mechanism

Thanks for participating…

QUESTIONS
&
ANSWERS