THE VALUE OF PERFORMANCE.
NORTHROP GRUMMAN

Cyber Security Workshop

DFARS Clause 252.204-7012 / NIST SP 800-171

20 December 2018

Prof. Clifford Neuman
Director, USC Center for Computer System Security

USC University of Southern California

Morning Agenda

NORTHROP GRUMMAN

8:00 – 9:30 AM Introduction and requirements

- Why are we here
- Legislation and Policy
  - DFARS and Executive Orders
  - CDI and CUI
  - Flow down requirements
  - Incident Reporting

9:45– Overview of Critical Controls in NIST SP 800-171

- What is “adequate security”
- What are the covered systems
- Risk Assessment and Risk Management
- High level coverage of critical controls in NIST SP 800-171
- Questions from Morning session

12 Noon – 1 PM Lunch

Afternoon Agenda

NORTHROP GRUMMAN

1 – 3 PM – Lightning Round Discussion: 110 Controls

- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical Security
- System and Communication protection
- System and Information Integrity

3:15 – 4 PM – Assessment and Security Plan

- Risk Assessment and Management
- Exostar tools for self assessment
- NIST System Security Plan

Afternoon Agenda Cont'd

NORTHROP GRUMMAN

4 - 4:30 PM Certifications and assessment methodologies
- Significance and types
- Best Practices

4:30 – 4:50 PM Questions and Discussion

4:50 – 5:00 PM Resources and Conclusion

THE VALUE OF PERFORMANCE.

NORTHROP GRUMMAN

Introduction and Requirements

Why are We Here

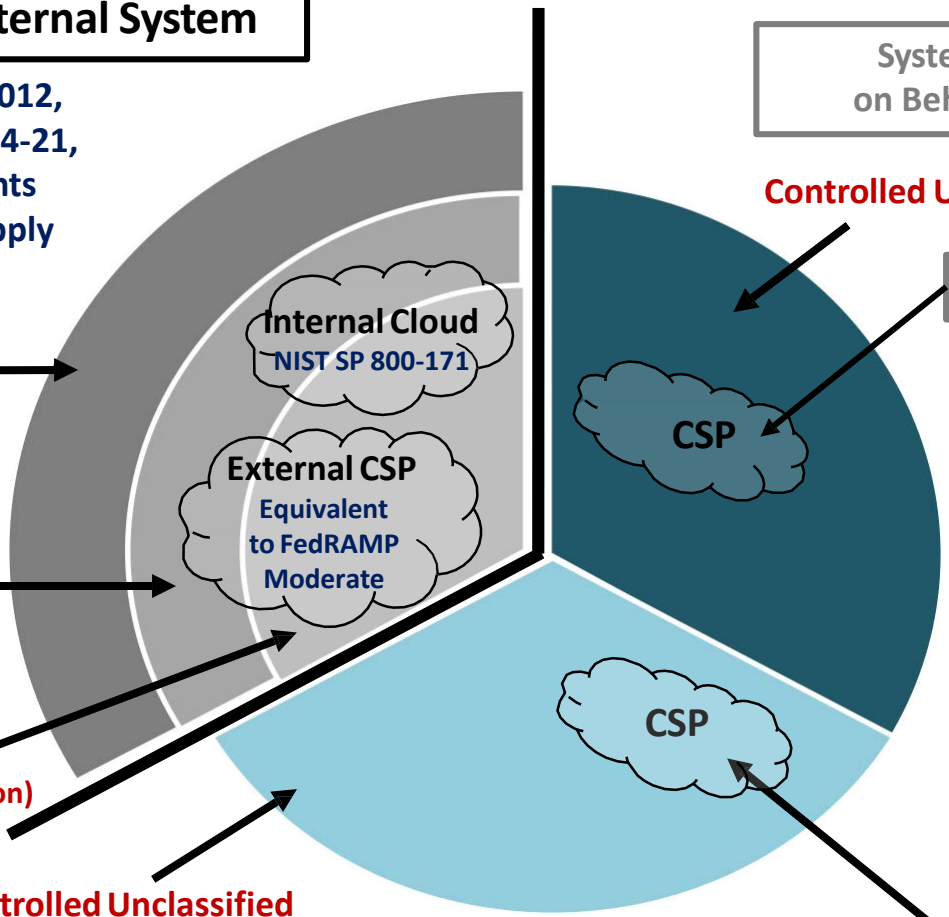
NORTHROP GRUMMAN

"**Why is cybersecurity important?**

Today, more than ever, the Department of Defense (DoD) relies upon external contractors to carry out a wide range of missions and shares sensitive data with these entities. Inadequate safeguards threaten America's national security and put servicemembers lives at risk."

-- US.DOD Office of Small Business Programs

Protecting the DoD's Unclassified Information



Contractor's Internal System

DFARS Clause 252.204-7012, and/or FAR Clause 52.204-21, and security requirements from NIST SP 800-171 apply

Federal Contract Information

Controlled Unclassified Information (USG-wide)

Covered Defense Information (includes Unclassified Controlled Technical Information)

Controlled Unclassified Information

System Operated on Behalf of the DoD

Controlled Unclassified Information

Cloud Service Provider

When cloud services are used to process data on the DoD's behalf, DFARS Clause 252.239-7010 and DoD Cloud Computing SRG apply

DoD Information System

Security requirements from CNSSI 1253, based on NIST SP 800-53, apply

Cloud Service Provider

When cloud services are provided by DoD, the DoD Cloud Computing SRG applies

DoD Owned and/or Operated Information System

Unclassified

Cyber Security Compliance Requirements

NORTHROP GRUMMAN

FAR 52.204-21

- **Basic Safeguarding of Covered Contractor Information Systems (Jun 2016)**
- 2014 and 2016 Implementation
- No Grace Period for Compliance
- 15 Controls (17 NIST)
- Considered Minimum Compliance Criteria
- Controlled Unclassified Information (CUI)

DFARS 252.204-7012

- **Safeguarding Covered Defense Information and Cyber Incident Reporting (Oct 2016)**
- Compliance or POAM required:
  - **30 Days from Award**
  - SSP + POAM is Compliant even if all 109 Controls not met
- **110 Controls (109 NIST + SSP/POAM)**
- Oct. 2016 Update added SSP & POAM Control to allow for Phase-in Period
- **Covered Defense Information (CDI)**

NIST SP 800-171

- **Special Publication: Protecting Unclassified Information in Nonfederal Information Systems and Organizations**
- Sets Industry Standard Practice
- **110 Controls (109 + SSP/POAM)**
  - Physical Site Controls
  - Computer System Controls
  - Process security controls

Safeguarding Covered Defense Information and Cyber Incident Reporting - DFARS Subpart 204.73

NORTHROP GRUMMAN

- DoD contractors (including small businesses) must:
  - Provide **adequate** security to safeguard ***covered defense information*** that resides in or transits through their internal unclassified information systems from unauthorized access and disclosure; and
  - Rapidly ***report cyber incidents (within 72 hours)*** and cooperate with DoD to respond to these security incidents, including access to affected media and submitting malicious software.

- Federal contracting officers are required to provide in each work statement or specification the identification of any covered defense information.

Source: https://www.acq.osd.mil/dpap/dars/dfars/html/current/204_73.htm

NORTHROP GRUMMAN

About Controlled Unclassified Information (CUI)

- ***Controlled Unclassified Information (CUI)*** is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is **not** classified under Executive Order 13526 or the Atomic Energy Act, as amended.

- Executive Order 13556 "Controlled Unclassified Information" (the Order), establishes a program for managing CUI across the Executive branch and designates the National Archives and Records Administration (NARA) as Executive Agent to implement the Order and oversee agency actions to ensure compliance. The Archivist of the United States delegated these responsibilities to the Information Security Oversight Office (ISOO).

- 32 CFR Part 2002 "Controlled Unclassified Information" was issued by ISOO 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.

NORTHROP GRUMMAN

About Covered Defense Information (CDI)

- While NIST 800-171 (discussed later) talks about Protecting ***Controlled Unclassified Information*** in Nonfederal Systems and Organizations, the DFARS require contractors to provide **adequate** security to safeguard ***covered defense information,*** that being so, what is the difference?
  - CDI is CUI. Additionally DoD has advised their major contractors to treat all CUI as CDI. Therefore you should treat the two terms as the same.
  - CDI is but one example of CUI. In explaining what steps must be taken to protect CUI, the NIST guidelines cover the protection of CDI as mandated by the DFARS.
  - Therefore all CUI (including CDI) must be protected in your covered contractor information systems.

NORTHROP GRUMMAN

About Covered Defense Information (CDI) Cont'd

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

NORTHROP GRUMMAN

About Covered Defense Information (CDI) Cont'd

- "***Technical information***" means technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013, Rights in Technical Data-Non Commercial Items, regardless of whether or not the clause is incorporated in this solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

- Primes **should** mark CDI provided to suppliers or note expected CDI to be developed in the contractual documents, but be sure to specifically ask your prime anyway.

NORTHROP GRUMMAN

What is a covered contractor information system

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

- The DFARS require contractors to provide adequate security on all covered contractor information systems.

- The definition of a "covered contractor information system" is critical in reducing the scope of effort by the contractor to ensure compliance with the adequate security requirement.
  - By providing separate security domains such that the majority of a contractors systems do not process, store, or transmit CDI, the contractor can focus their compliance efforts on the smaller subset of their system that do.
  - Of course contractors have other reasons to ensure that all parts of their systems have adequate security. But this effectively reduces the "attack surface" for the CDI itself.

NORTHROP GRUMMAN

What Security Measures are "Adequate"?

- No systems are completely secure
- Government systems are being breached all the time.
  - Do these systems provide "adequate" security to safeguard the information they process?
  - Certainly they were not sufficient to prevent these breaches.
  - Example: Breach at the Office of Personnel Management.
- But, according to the DFARS:

" A cyber incident that is reported by a contractor or subcontractor shall not, by itself, be interpreted as evidence that the contractor or subcontractor has failed to provide adequate security on their covered contractor information systems, or has otherwise failed to meet the requirements of the clause at 252.204-7012"

NORTHROP GRUMMAN

What Security Measures are “Adequate”? Cont'd

- But can we really define “adequate” retrospectively?
  - Your security was not adequate if you did not employ industry and sector appropriate measures.
  - Your security was not adequate if you did not have a plan to secure your systems
  - Your security was not adequate if you did not perform a risk assessment.
- If you did all of these and still were breached, then the answer is less clear.
- NIST SP 800-171 describes good practices that must be followed. If they are not followed, then your security measures are definitely not “Adequate”.

NORTHROP GRUMMAN

Cyber Incident Reporting

- Contractors and subcontractors must **report cyber incidents** on covered information systems with CDI, *or that affect the ability to perform operationally critical support* under a contract
  - Upon discovery must conduct a review for evidence of compromise
  - Rapidly report within 72 hours directly to DoD via specified online portal
  - Must provide DoD-assigned incident report number to prime/higher tiered subcontractor
  - Must preserve and protect images of known affected images and systems for 90 days
  - Must provide DoD access to additional information or equipment necessary to conduct forensics analysis
  - Must submit any malicious software you uncover to DoD Cyber Crime Center (C3), not the Contracting Officer

NORTHROP GRUMMAN

Response to a Cyber-Incident

- Reporting of a breach of a covered system is required as described on the previous slide.
- An assessment of the breach must identify those systems affected, and the covered defense information and other controlled unclassified information that could have potentially been released.
  - If appropriate auditing and intrusion detection components were in place, that may involve identifying the specific data that was accessed or exfiltrated.
  - Otherwise, it must identify all potential information that could have been accessible to the adversary or malicious code affecting your system.

NORTHROP GRUMMAN

Response to a Cyber-Incident Cont'd

- In responding to a cyber-incident:
  - Steps must be taken to contain the attack and prevent further disclosure of CDI and CUI. This may involve disconnecting the system from the network, and potentially shutting down the system.
  - Any malicious software found on your system must be preserved and provided to investigating authorities.
  - Logs and records from your system must be preserved to enable forensic analysis of the attack.

NORTHROP GRUMMAN

Verification of Your Identity

External Certification Authority Program:

- The DoD has established the External Certification Authority (ECA) program to support the issuance of DoD-approved certificates to industry partners and other external entities and organizations. The ECA program is designed to provide the mechanism for these entities to securely communicate with the DoD and authenticate to DoD Information Systems.

- You will need to obtain:
  - Medium Level Assurance Certificate
    - http://iase.disa.mil/pki/eca/Pages/index.aspx.

This is NOT certification that your systems meets any program requirements. This merely certifies identity.

NORTHROP GRUMMAN

What to Do

- Understand what Federal Contract Information (FCI), Controlled Unclassified Information (CUI) or Covered Defense Information (CDI) is included in your contracts
- Understand the controls in NIST SP 800-171 (this class)
- Have an internal discussion regarding adequate security needed for the FCI, CDI & CDI
- Complete the self-assessment questionnaire. As part of this assessment (as described later):
  - Complete a Risk Assessment (3.11.1)
  - Develop a System Security Plan (3.12.4)
  - Develop a plan of action and milestones (3.12.2)
- Flow-down requirement to suppliers at all tiers

What Contracts, Contractors, and Subs are Impacted

NORTHROP GRUMMAN

- All federal contracts are impacted except for solicitations and contracts solely for COTS (Common off the shelf technologies) items

- 204.7304 Solicitation provision and contract clauses.

  (a) Use the provision at 252.204-7008, ***Compliance with Safeguarding Covered Defense Information Controls***, in all solicitations, including solicitations using FAR part 12 procedures for the acquisition of commercial items, except for solicitations solely for the acquisition of commercially available off-the-shelf (COTS) items

  (b) Use the clause at 252.204-7009, ***Limitations on the Use or Disclosure of Third- Party Contractor Reported Cyber Incident Information***, in all solicitations and contracts, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial items, for services that include support for the Government's activities related to safeguarding covered defense information and cyber incident reporting

  (c) Use the clause at 252.204-7012, ***Safeguarding Covered Defense Information and Cyber Incident Reporting***, in all solicitations and contracts, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial items, except for solicitations and contracts solely for the acquisition of COTS items.

Flow-Down Requirements

NORTHROP GRUMMAN

- The DFAR requirements for adequate security must flow down to all tiers.
  - From prime to sub-contractors
  - From sub-contractors to sub subs, etc.
  - To anyone that will process, store, or transmits covered defense information.
  - This includes vendors and providers of IT systems and services.

NORTHROP GRUMMAN

Review of Common Implementation Steps

- Understand what Federal Contract Information (FCI), Controlled Unclassified Information (CUI) or Covered Defense Information (CDI) is included in your contracts
- Complete a self-assessment
- Flow-down requirement to suppliers at all tiers

NORTHROP GRUMMAN

What about the Cloud

- Many small businesses necessarily use cloud services to support their day to day operations. Can the cloud be used to process CDI and CUI.
  - Some providers may claim compliance to NIST SP 800-171 (or other NIST standards, for PCI standards or HIPAA standards) – what does this mean.
    - Don't believe that by using such "compliant" cloud systems that your handling of CDI is automatically compliant.
    - You must ensure (contractually with the vendor) that the specific systems they are providing meet the flow down requirements. (You may need to pay extra for the segregated and compliant servers).
    - You must also ensure that the communication and local processing of such data by your own systems, and by your applications that run on the cloud services are similarly compliant.
  - See FEDRAMP for an example of how the government accredits and contracts for such services.

One example

NORTHROP GRUMMAN

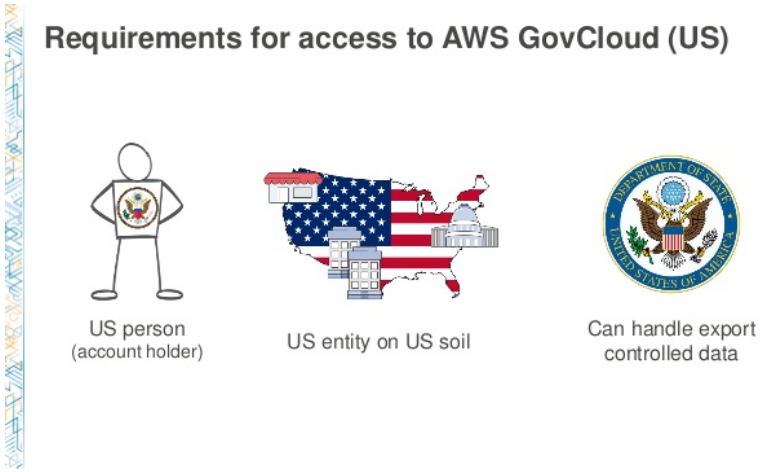
AWS GovCloud (US) Region

Designed to address the specific regulatory needs of United States federal, state and local agencies, education institutions and the supporting ecosystem.

AWS GovCloud (US)

AWS GovCloud (US) Region:

- Subject to FedRAMP High and Moderate baselines
- Allow customers to host sensitive Controlled Unclassified Information (CUI) and all types of regulated workloads
- Operated by employees who are U.S. citizens on U.S. soil
- Only accessible to vetted U.S. entities and root account holders, who must confirm they are U.S. Persons to gain access



One example

NORTHROP GRUMMAN

Addresses Security & Compliance

Gives vetted government customers and their partners the **flexibility to architect** secure cloud solutions that comply with:

Federal Risk and Authorization Management Program (FedRAMP) Moderate and **High. Learn	Federal Information Security Management Act (FISMA) Low, Moderate and **High	Department of Defense Security Requirements Guide (SRG) Impact Levels 2, **4 and **5. Learn more.	U.S. International Traffic in Arms Regulations (ITAR)	**Department of Commerce Export Administration Regulations (EAR)	**IRS-1075 Encryption Standards for Federal Tax Information (FTI) Section 6103 (p)
**Department of Justice Criminal Justice Information Service Security Policy	**National Institute of Standards and Technology (NIST) SP 800--53 (rev4) and SP 800-171	**Federal Information Processing Standard Publication	**Defense Federal Acquisition Regulation Supplement (DFARS)	Healthcare Insurance Portability & Accountability Act Privacy Standards	Payment Card Industry Security Standards

Other Vendors may provide similar services and it is up to you to validate the accreditation of such services (including this example).

THE VALUE OF PERFORMANCE.

NORTHROP GRUMMAN

Overview of the critical controls in NIST SP 800-171

“The Critical Seventeen”

NORTHROP GRUMMAN

The Critical Seventeen

- NIST SP 800-171 list 110 controls that correspond to industry best practices. In this session we will discuss the seventeen most critical of those controls.

- These seventeen must be implemented NOW on all covered contractor information systems, as mandated by the FARs.

- This afternoon we will discuss these controls again, in the context of the full set of 110 controls from NIST SP 800-171 which you should implement as soon as possible, and for which you **must** have a plan of action and milestones in place.

NIST SP 800-171
Minimum Cyber-Security Standards

NORTHROP GRUMMAN

- NIST SP 800-171: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
  - Lists 110 requirements in 14 areas

Access Control	Media Protection
Awareness & Training	Personnel Security
Audit & Accountability	Physical Protection
Configuration Management	Risk Assessment
Identification & Authentication	Security Assessment
Incident Response	System & Com Protection
Maintenance	System & Info Integrity

- For the rest of the morning we will focus on a subset of 17 of these requirements/controls, then in the afternoon we will circle back and cover all 110 controls.

Access Control and Identity Management

NORTHROP GRUMMAN

FAR Clause 52.204-21(b)(1)	NIST 800-171 Reference	Basic or Derived	800-171 Family
(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	3.1.1	Basic	Access Control
(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	3.1.2	Basic	Access Control
(iii) Verify and control/limit connections to, and use of, external information systems.	3.1.20	Derived	Access Control
(iv) Control information posted or processed on publicly accessible information systems.	3.1.22	Derived	Access Control
(v) Identify information system users, processes acting on behalf of users, or devices.	3.5.1	Basic	Identification and Authentication
(vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	3.5.2	Basic	Identification and Authentication

Cyber Perimeter

NORTHROP GRUMMAN

(i) Limit information system access to:

- authorized users,
- processes acting on behalf of authorized users,
- or devices (including other information systems)

Methods:

Account Management
Firewalls
Limits to BYOD
Network Access Control
Remote access limitations

SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.1 ACCESS CONTROL				
Basic Security Requirements				
3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other systems). 3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute.	AC-2	Account Management	A.9.2.1	User registration and de-registration
			A.9.2.2	User access provisioning
			A.9.2.3	Management of privileged access rights
			A.9.2.5	Review of user access rights
			A.9.2.6	Removal or adjustment of access rights
	AC-3	Access Enforcement	A.6.2.2	Teleworking
			A.9.1.2	Access to networks and network services
			A.9.4.1	Information access restriction
			A.9.4.4	Use of privileged utility programs
			A.9.4.5	Access control to program source code
			A.13.1.1	Network controls
			A.14.1.2	Securing application services on public networks
			A.14.1.3	Protecting application services transactions
			A.18.1.3	Protection of records
	AC-17	Remote Access	A.6.2.1	Mobile device policy
			A.6.2.2	Teleworking
			A.13.1.1	Network controls
			A.13.2.1	Information transfer policies and procedures
			A.14.1.2	Securing application services on public networks
Derived Security Requirements				

Least Privilege

NORTHROP GRUMMAN

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

Methods:

Privileged accounts
Access Controls
Information Flow Constraints
Separate server accounts

Breaches:
SF Muni Hack
Hollywood Presb Hospital
Most major ransomware

SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.1 ACCESS CONTROL				
Basic Security Requirements				
3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other systems). **3.1.2** Limit system access to the types of transactions and functions that authorized users are permitted to execute.	AC-2	Account Management	A.9.2.1	User registration and de-registration
			A.9.2.2	User access provisioning
			A.9.2.3	Management of privileged access rights
			A.9.2.5	Review of user access rights
			A.9.2.6	Removal or adjustment of access rights
	AC-3	Access Enforcement	A.6.2.2	Teleworking
			A.9.1.2	Access to networks and network services
			A.9.4.1	Information access restriction
			A.9.4.4	Use of privileged utility programs
			A.9.4.5	Access control to program source code
			A.13.1.1	Network controls
			A.14.1.2	Securing application services on public networks
			A.14.1.3	Protecting application services transactions
			A.18.1.3	Protection of records
	AC-17	Remote Access	A.6.2.1	Mobile device policy
			A.6.2.2	Teleworking
			A.13.1.1	Network controls
			A.13.2.1	Information transfer policies and procedures
			A.14.1.2	Securing application services on public networks
Derived Security Requirements				

Containment

NORTHROP GRUMMAN

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

3.1.20 Verify and control/limit connections to and use of external systems.	AC-20	Use of External Systems	A.11.2.6	Security of equipment and assets off-premises
			A.13.1.1	Network controls
			A.13.2.1	Information transfer policies and procedures
	AC-20(1)	Use of External Systems *Limits on Authorized Use*	*No direct mapping.*	

Prevent Exfiltration

How the data gets out

Could be as simple as apparent web access

Other basic internet services

Definitely SFTP and FTP

Impose policies on use

But what is external?

Examples of Breaches:

- Use of hacked Samsung TVs
- Target
- Home Depot
- Equifax
- HBO
- Sony

Stay within the Perimeter

NORTHROP GRUMMAN

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

3.1.22	Control CUI posted or processed on publicly accessible systems.	AC-22	Publicly Accessible Content	*No direct mapping.*

What are “publicly accessible information systems”?

- Your public web server
- Can include any webserver that might be mis-configured to serve data from folders that should be protected
- Can include uploading data to wrong directories

The Cloud

- Amazon S3 Lockers
- Dropbox and similar services
- Gmail and other alternative communications services, e.g. Yahoo

Could also be your employees home machines or laptops

Attribution and Identification

NORTHROP GRUMMAN

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

SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.5 IDENTIFICATION AND AUTHENTICATION				
Basic Security Requirements				
3.5.1 Identify system users, processes acting on behalf of users, or devices.	IA-2	Identification and Authentication (Organizational Users)	A.9.2.1	User registration and de-registration
3.5.2 Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational systems.	IA-5	Authenticator Management	A.9.2.1	User registration and de-registration
			A.9.2.4	Management of secret authentication information of users
			A.9.3.1	Use of secret authentication information
			A.9.4.3	Password management system

Where:

In log files

In the system itself, for use in access decisions.

No group accounts.

Authentication

NORTHROP GRUMMAN

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

SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.5 IDENTIFICATION AND AUTHENTICATION				
Basic Security Requirements				
3.5.1 Identify system users, processes acting on behalf of users, or devices.	IA-2	Identification and Authentication (Organizational Users)	A.9.2.1	User registration and de-registration
3.5.2 Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational systems.	IA-5	Authenticator Management	A.9.2.1	User registration and de-registration
			A.9.2.4	Management of secret authentication information of users
			A.9.3.1	Use of secret authentication information
			A.9.4.3	Password management system

Plus a whole bunch of derived controls that tell us how to do this one effectively.

Methods: Strong Passwords (and policies)
Second Factors (cards, biometrics)

More on Authentication

NORTHROP GRUMMAN

While not within the 17 primary elements we focus on this morning, these provide good advice on how to perform 3.5.2 effectively.

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.	IA-2(1)	Identification and Authentication (Organizational Users) *Network Access to Privileged Accounts*	*No direct mapping.*		
	IA-2(2)	Identification and Authentication (Organizational Users) *Network Access to Non-Privileged Accounts*	*No direct mapping.*		
	IA-2(3)	Identification and Authentication (Organizational Users) *Local Access to Privileged Accounts*	*No direct mapping.*		
3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	IA-2(8)	Identification and Authentication (Organizational Users) *Network Access to Privileged Accounts-Replay Resistant*	*No direct mapping.*		
	IA-2(9)	Identification and Authentication (Organizational Users) *Network Access to Non-Privileged Accounts-Replay Resistant*	*No direct mapping.*		
3.5.5 Prevent reuse of identifiers for a defined period.	IA-4	Identifier Management	A.9.2.1	User registrati de-registratio	

SECURITY REQUIREMENTS		NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.5.6	Disable identifiers after a defined period of inactivity.	IA-4	Identifier Management	A.9.2.1	User registration and de-registration
3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	IA-5(1)	Authenticator Management *Password-Based Authentication*	*No direct mapping.*	
3.5.8	Prohibit password reuse for a specified number of generations.				
3.5.9	Allow temporary password use for system logons with an immediate change to a permanent password.				
3.5.10	Store and transmit only cryptographically-protected passwords.				
3.5.11	Obscure feedback of authentication information.	IA-6	Authenticator Feedback	A.9.4.2	Secure logon procedures

Physical, Media, and Communications

NORTHROP GRUMMAN

(vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.	3.8.3	Basic	Media Protection
(viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	3.10.1	Basic	Physical Protection
(ix) Escort visitors and monitor visitor activity… …maintain audit logs of physical access, and… …control and manage physical access devices.	3.10.3 3.10.4 3.10.5	Derived	Physical Protection
(x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	3.13.1	Basic	System and Communication Protection
(xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	3.13.5	Derived	System and Communication Protection

Seek out and Destroy

NORTHROP GRUMMAN

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

What is this media:

- CDs or DVD's
- Thumb Drives
- Hard drives inside computers
- Copy machines
- Printers
- Printouts
- Cellphones
- SSD's

SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.8 MEDIA PROTECTION				
Basic Security Requirements				
3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. 3.8.2 Limit access to CUI on system media to authorized users. 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse.	MP-2	Media Access	A.8.2.3	Handling of Assets
			A.8.3.1	Management of removable media
			A.11.2.9	Clear desk and clear screen policy
	MP-4	Media Storage	A.8.2.3	Handling of Assets
			A.8.3.1	Management of removable media
			A.11.2.9	Clear desk and clear screen policy
	MP-6	Media Sanitization	A.8.2.3	Handling of Assets
			A.8.3.1	Management of removable media
			A.8.3.2	Disposal of media
			A.11.2.7	Secure disposal or reuse of equipment

What about encrypted drives.
e.g. Whole disk encryption
Other forms of encryption

Physical Access

NORTHROP GRUMMAN

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

How easy would it be for someone to plug a USB device into one of your systems.

SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.10 PHYSICAL PROTECTION				
Basic Security Requirements				
3.10.1 Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.	PE-2	Physical Access Authorizations	A.11.1.2*	Physical entry controls
	PE-5	Access Control for Output Devices	A.11.1.2	Physical entry controls
			A.11.1.3	Securing offices, rooms, and facilities
3.10.2 Protect and monitor the physical facility and support infrastructure for organizational systems.	PE-6	Monitoring Physical Access	*No direct mapping.*	

How about placing a cell phone on the table next to your keyboard. Wherever your authorized users conduct work must be thought of as the respective operating environment.

Visibility of input and output devices from beyond the perimeter.

Building Access

NORTHROP GRUMMAN

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

Derived Security Requirements				
3.10.3 Escort visitors and monitor visitor activity.	PE-3	Physical Access Control	A.11.1.1	Physical security perimeter
			A.11.1.2	Physical entry controls
3.10.4 Maintain audit logs of physical access.			A.11.1.3	Securing offices, rooms, and facilities
3.10.5 Control and manage physical access devices.				

Physical access devices:

- Metal keys (hard to manage 3.10.4)
- Proximity cards (can be copied) – can require passcode too, still not perfect
- Locks – manage centrally based on identity of authorized individuals

Cyber Perimeter Monitoring/Control

NORTHROP GRUMMAN

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

- Firewalls
  - rules
- VLANs
- Network architecture
- VPNs
- Network access controls
- Security for WiFi and physical network ports

SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.13 SYSTEM AND COMMUNICATIONS PROTECTION				
Basic Security Requirements				
3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	SC-7	Boundary Protection	A.13.1.1	Network controls
			A.13.1.3	Segregation in networks
			A.13.2.1	Information transfer policies and procedures
			A.14.1.3	Protecting application services transactions
3.13.2 Employ architectural				

Guests and the DMZ

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

Multiple networks

Not just VLANs

3.13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	SC-7	Boundary Protection	A.13.1.1	Network controls
			A.13.1.3	Segregation in networks
			A.13.2.1	Information transfer policies and procedures
			A.14.1.3	Protecting application services transactions

Consider 3 or 4

- Operational network for those needing access to CUI
- Operational network for your other employees – still protects your company's other assets
- Optional third network if you need to provide "guest" access – only communicates to outside.
- Public facing servers can go on 4th network in the "DMZ" between public and NON-CUI network

System Integrity and Subversion

NORTHROP GRUMMAN

(xii) Identify, report, and correct information and information system flaws in a timely manner.	3.14.1	Basic	System and Information Integrity
(xiii) Provide protection from malicious code at appropriate locations within organizational information systems.	3.14.3	Basic	System and Information Integrity
(xiv) Update malicious code protection mechanisms when new releases are available.	3.14.2	Derived	System and Information Integrity
(xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	3.14.5	Derived	System and Information Integrity

Patching and Sharing

NORTHROP GRUMMAN

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

Patches

e.g. Equifax

To patch or not to patch:

e.g. cCleaner, Peyta

Malware hitched rides on software updates.

Conclusion – Know your updates.

SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.14 SYSTEM AND INFORMATION INTEGRITY				
Basic Security Requirements				
3.14.1 Identify, report, and correct information and system flaws in a timely manner. **3.14.2** Provide protection from malicious code at appropriate locations within organizational systems. **3.14.3** Monitor system security alerts and advisories and take appropriate actions in response.	SI-2	Flaw Remediation	A.12.6.1	Management of technical vulnerabilities
			A.14.2.2	System change control procedures
			A.14.2.3	Technical review of applications after operating platform changes
			A.16.1.3	Reporting information security weaknesses
	SI-3	Malicious Code Protection	A.12.2.1	Controls against malware
	SI-5	Security Alerts, Advisories, and Directives	A.6.1.4*	Contact with special interest groups

- Vulnerability and breach reporting.
  - 72 hours

Antivirus and More

NORTHROP GRUMMAN

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

Protection =

- Anitvirus
- Anti-malware
- Isolated execution environments
- Least privilege
- Network isolation

SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.14 SYSTEM AND INFORMATION INTEGRITY				
Basic Security Requirements				
3.14.1 Identify, report, and correct information and system flaws in a timely manner. **3.14.2** Provide protection from malicious code at appropriate locations within organizational systems. **3.14.3** Monitor system security alerts and advisories and take appropriate actions in response.	SI-2	Flaw Remediation	A.12.6.1	Management of technical vulnerabilities
			A.14.2.2	System change control procedures
			A.14.2.3	Technical review of applications after operating platform changes
			A.16.1.3	Reporting information security weaknesses
	SI-3	Malicious Code Protection	A.12.2.1	Controls against malware
	SI-5	Security Alerts, Advisories, and Directives	A.6.1.4*	Contact with special interest groups

AV and Attack Signatures

NORTHROP GRUMMAN

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

Derived Security Requirements				
3.14.4 Update malicious code protection mechanisms when new releases are available.	SI-3	Malicious Code Protection	A.12.2.1	Controls against malware
3.14.5 Perform periodic scans of				

- We all know this right?
- What if you are using Kaspersky?

As with any software – some update types can carry malicious code.

Apply Live AV and Scanning

NORTHROP GRUMMAN

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

Scans of system:

- AV
- Tripwire or AFIK
- Check integrity

Derived Security Requirements				
3.14.4 Update malicious code protection mechanisms when new releases are available.	SI-3	Malicious Code Protection	A.12.2.1	Controls against malware
3.14.5 Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.				

As files are downloaded, opened, or executed

- Most AV systems will do this
- But, also apply scanning in servers and proxies (email, web proxies, firewalls)

Intrusion Detection

NORTHROP GRUMMAN

- Beyond the Critical 17 covered this morning, consider network-based intrusion detection tools.

3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	SI-4	System Monitoring	*No direct mapping.*
		SI-4(4)	System Monitoring *Inbound and Outbound Communications Traffic*	*No direct mapping.*
3.14.7	Identify unauthorized use of organizational systems.	SI-4	System Monitoring	*No direct mapping.*

- Some subversions detectable through command and control detection.
- Consider detection based on your knowledge of partners – what communication is odd (anomalous)

Risk Assessment and Security Plan

NORTHROP GRUMMAN

- Start with a list of all your assets, especially CDI, FCI, and CUI. Where is it resident on your systems.
  - Who needs access, and who does not.
  - Can you segregate parts of the system needing CUI.
- Assess the controls in place on each of your system components against at least the 17 controls discussed this morning..
  - What's missing – i.e. what don't you meet.
  - What do you need to do to meet these requirements
  - Are there interim steps you can take (e.g. segregation – don't process CUI on some systems).
- Complete an IT Security Plan
  - This will be covered this afternoon.

Questions on material from morning

NORTHROP GRUMMAN

THE VALUE OF PERFORMANCE.
NORTHROP GRUMMAN

Lightning Round Discussion of all 110 Controls in NIST SP 800-171

(Assessment and security plan covered later)

NIST SP 800-171 Controls
What to Expect

NORTHROP GRUMMAN

- Most Government and Prime Contractor Customers will require supplier Assertions regarding which of the 110 controls in NIST SP 800-171 are fully **implemented** in your organization.
  - You MUST implement at least the critical 17.
  - You must have performed a security assessment.
  - You MUST have a plan of action and milestones for the remaining controls.

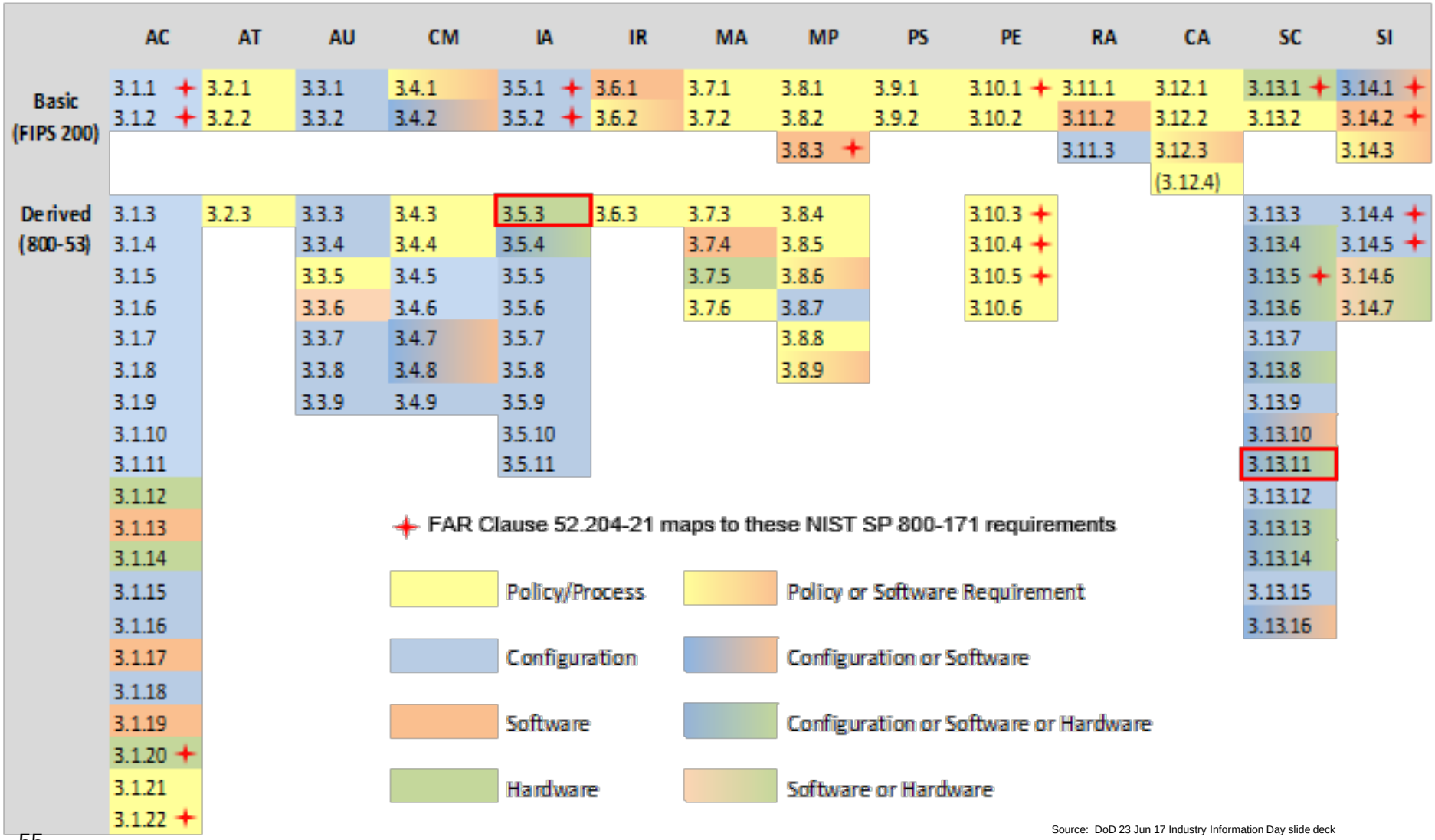
- What does fully implemented mean?
  - You have processes in place to ensure that the control is met
    - And that you honestly consider the process that is in place to be sufficient (adequate)
  - It does not mean that the process is fool-proof

- Different ways to meet the control:
  - Configuration, Hardware, Software, or Policy
  - Policy may simply involve not using systems for certain purposes

- Many of the controls remaining from the 110 are refinements to the critical 17 (e.g. dictating specific ways to meet the critical 17).

Implementing NIST SP 800-171 (R1)

NORTHROP GRUMMAN



Source: DoD 23 Jun 17 Industry Information Day slide deck

AIA members noted hardest and costliest

Set 3.1 - Access Control

NORTHROP GRUMMAN

Which of the following NIST SP 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company.

- 3.1.1. Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other systems).
- 3.1.2. Limit system access to the types of transactions and functions that authorized users are permitted to execute.
- 3.1.3. Control the flow of CUI in accordance with approved authorizations.
- 3.1.4. Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
- 3.1.5. Employ the principle of least privilege, including for specific security functions and privileged accounts.
- 3.1.6. Use non-privileged accounts or roles when accessing nonsecurity functions.

LEAST PRIVILEGE

Set 3.1 - Access Control Cont'd

NORTHROP GRUMMAN

Which of the following NIST SP 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company.

Access control and privilege policy

Notice of policy

Autologout / lock

- 3.1.7. Prevent non-privileged users from executing privileged functions and audit the execution of such functions.
- 3.1.8. Limit unsuccessful logon attempts.
- 3.1.9. Provide privacy and security notices consistent with applicable CUI rules.
- 3.1.10. Use session lock with pattern-hiding displays to prevent access and viewing of data after period of inactivity.
- 3.1.11. Terminate (automatically) a user session after a defined condition.

Set 3.1 - Access Control (b)

NORTHROP GRUMMAN

Which of the following NIST SP 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company.

- 3.1.12. Monitor and control remote access sessions.
- 3.1.13. Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
- 3.1.14. Route remote access via managed access control points.
- 3.1.15. Authorize remote execution of privileged commands and remote access to security- relevant information.
- 3.1.16. Authorize wireless access prior to allowing such connections.
- 3.1.17. Protect wireless access using authentication and encryption.
- 3.1.18. Control connection of mobile devices.
- 3.1.19. Encrypt CUI on mobile devices and mobile computing platforms.

Set 3.1 - Access Control (b) Cont'd

NORTHROP GRUMMAN

Which of the following NIST SP 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company.

- 3.1.20. Verify and control/limit connections to and use of external systems.
- 3.1.21. Limit use of organizational portable storage devices on external systems.
- 3.1.22. Control CUI posted or processed on publicly accessible systems.

Manage remote access

Manage data on remote/mobile devices
Controls on portable storage

Control of information on publicly accessible servers.

Set 3.2 Awareness and Training

NORTHROP GRUMMAN

Which of the following NIST SP 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company.

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

Set 3.3 Audit and Accountability

NORTHROP GRUMMAN

Which of the following NIST SP 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company.

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

- 3.3.2. Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.
- 3.3.3. Review and update audited events.
- 3.3.4. Alert in the event of an audit process failure.
- 3.3.5. Use automated mechanisms to integrate and correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.
- 3.3.6. Provide audit reduction and report generation to support on-demand analysis and reporting.

Manage system logs

Protecting them
Monitoring them
What they contain
Alert on log failure
Automated tools
Common time base
Who managed logs

Set 3.3 Audit and Accountability

NORTHROP GRUMMAN

Which of the following NIST SP 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company.

- 3.3.7. Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.
- 3.3.8. Protect audit information and audit tools from unauthorized access, modification, and deletion.
- 3.3.9. Limit management of audit functionality to a subset of privileged users.

Manage system logs

Protecting them
Monitoring them
What they contain
Alert on log failure
Automated tools
Common time base
Who managed logs

Set 3.4 Configuration Management

NORTHROP GRUMMAN

Which of the following NIST SP 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company.

- 3.4.1. Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.
- 3.4.2. Establish and enforce security configuration settings for information technology products employed in organizational systems.
- 3.4.3. Track, review, approve/disapprove, and audit changes to organizational systems.
- 3.4.4. Analyze the security impact of changes prior to implementation.
- 3.4.5. Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational system.
- 3.4.6. Employ the principle of least functionality by configuring organizational system to provide only essential capabilities.

Set 3.4 Configuration Management Cont'd

NORTHROP GRUMMAN

Which of the following NIST SP 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company.

- 3.4.7. Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.
- 3.4.8. Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.
- 3.4.9. Control and monitor user-installed software.

Manage the software, hardware and configurations of the systems running on your network.

Set 3.5 Identification and Authentication

NORTHROP GRUMMAN

Which of the following NIST SP 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company.

- 3.5.1. Identify system users, processes acting on behalf of users, or devices.
- 3.5.2. Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational systems.
- 3.5.3. Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
- 3.5.4. Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.
- 3.5.5. Prevent reuse of identifiers for a defined period.
- 3.5.6. Disable identifiers after a defined period of inactivity.
- 3.5.7. Enforce a minimum password complexity and change of characters when new passwords are created.

Set 3.5 Identification and Authentication Cont'd

NORTHROP GRUMMAN

Which of the following NIST SP 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company.

- 3.5.8. Prohibit password reuse for a specified number of generations.
- 3.5.9. Allow temporary password use for system logons with an immediate change to a permanent password.
- 3.5.10. Store and transmit only cryptographically-protected passwords.
- 3.5.11. Obscure feedback of authentication information.

Multi-factor authentication
Password Policies
How passwords entered
Resistance to various attacks

Set 3.6 Incident Response

NORTHROP GRUMMAN

Which of the following NIST SP 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company.

- 3.6.1. Establish an operational incident-handling capability for organizational systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.
- 3.6.2. Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization.
- 3.6.3. Test the organizational incident response capability.

3.6.1 (and 3.6.3) is a 3 hour lecture in and of itself.

3.6.2 follows from the plan.

This will be good for your organization in general, independent of the CUI requirements.

But it will be time and labor intensive.

Set 3.7 Maintenance

NORTHROP GRUMMAN

Which of the following NIST SP 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company.

- 3.7.1. Perform maintenance on organizational systems.
- 3.7.2. Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.
- 3.7.3. Ensure equipment removed for off-site maintenance is sanitized of any CUI.
- 3.7.4. Check media containing diagnostic and test programs for malicious code before the media are used in organizational system.
- 3.7.5. Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.
- 3.7.6. Supervise the maintenance activities of maintenance personnel without required access authorization.

Remove disks before sending equipment back for repair.

Easier said than done.

Equipment maintenance personnel need to be supervised.

Remote desktop for maintenance is problematic.

Set 3.8 Media Protection

NORTHROP GRUMMAN

Which of the following NIST SP 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company.

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

Manage, Label, Control access to, and Encrypt media and destroy in appropriate manner.

- 3.8.2. Limit access to CUI on system media to authorized users.
- 3.8.3. Sanitize or destroy system media containing CUI before disposal or release for reuse.
- 3.8.4. Mark media with necessary CUI markings and distribution limitations
- 3.8.5. Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.
- 3.8.6. Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

Set 3.8 Media Protection Cont'd

NORTHROP GRUMMAN

Which of the following NIST SP 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company.

- 3.8.7. Control the use of removable media on system components.
- 3.8.8. Prohibit the use of portable storage devices when such devices have no identifiable owner.
- 3.8.9. Protect the confidentiality of backup CUI at storage locations

Manage, Label, Control access to, and Encrypt media and destroy in appropriate manner.

Set 3.9 Personnel Security

NORTHROP GRUMMAN

Which of the following NIST SP 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company.

- 3.9.1. Screen individuals prior to authorizing access to organizational systems containing CUI.

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

Set 3.10 Physical Protection

NORTHROP GRUMMAN

Which of the following NIST SP 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company.

- 3.10.1. Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.
- 3.10.2. Protect and monitor the physical facility and support infrastructure for organizational systems
- 3.10.3. Escort visitors and monitor visitor activity.
- 3.10.4. Maintain audit logs of physical access.
- 3.10.5. Control and manage physical access devices.
- 3.10.6. Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites).

Set 3.13 System and Comm Protection

NORTHROP GRUMMAN

Which of the following NIST SP 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company.

- 3.13.1. Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.
- 3.13.2. Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.
- 3.13.3. Separate user functionality from system management functionality.
- 3.13.4. Prevent unauthorized and unintended information transfer via shared system resources.
- 3.13.5. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

Set 3.13 System and Comm Protection Cont'd

NORTHROP GRUMMAN

Which of the following NIST SP 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company.

- 3.13.6. Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).
- 3.13.7. Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks.
- 3.13.8. Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.
- 3.13.9. Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.
- 3.13.10. Establish and manage cryptographic keys for cryptography employed in organizational systems.

Set 3.13 System and Comm Protection Cont'd

NORTHROP GRUMMAN

Which of the following NIST SP 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company.

- 3.13.11. Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. (for now this means AES and appropriate PK systems)
- 3.13.12. Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.
- 3.13.13. Control and monitor the use of mobile code.
- 3.13.14. Control and monitor the use of Voice over Internet Protocol (VoIP) technologies
- 3.13.15. Protect the authenticity of communications sessions
- 3.13.16. Protect the confidentiality of CUI at rest.

Set 3.14 System & Information Integrity

NORTHROP GRUMMAN

Which of the following NIST SP 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company.

- 3.14.1. Identify, report, and correct information and system flaws in a timely manner.
- 3.14.2. Provide protection from malicious code at appropriate locations within organizational systems.
- 3.14.3. Monitor system security alerts and advisories and take appropriate actions in response.
- 3.14.4. Update malicious code protection mechanisms when new releases are available.
- 3.14.5. Perform periodic scans of organizational system and real-time scans of files from external sources as files are downloaded, opened, or executed.
- 3.14.6. Monitor organizational system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.
- 3.14.7. Identify unauthorized use of organizational system

Risk Assessment and Security Plan

NORTHROP GRUMMAN

- Start with a list of all your assets, especially CDI, FCI, and CUI. Where is it resident on your systems.
  - Who needs access, and who does not.
  - Can you segregate parts of the system needing CUI.

- Assess the controls in place on each of your system components against the 110 controls in NIST SP 800-171.
  - What's missing – i.e. what don't you meet.
  - What do you need to do to meet these requirements
  - Are there interim steps you can take (e.g. segregation – don't process CUI on some systems).

- Complete an IT Security Plan
  - This will be a focus in our second week

Set 3.11 Risk Assessment

NORTHROP GRUMMAN

Which of the following NIST SP 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company.

- 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.

DEFINE YOUR PERIMETER

- 3.11.2 Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified.

- 3.11.3 Remediate vulnerabilities in accordance with assessments of risk.

Risk Management

NORTHROP GRUMMAN

The goal of security in all organization is to manage risk. The first step in managing risk is your risk assessment (3.11.1)

Once risks are assessed, characterized, and quantified, your organization takes steps to mitigate those risks, balancing the cost of the mitigation against the potential loss resulting from the risk.

In the case of CDI, the requirements are that you apply adequate (e.g. industry best practices as identified in NIST SP 800-171) to mitigate all identified risks to CDI from your risk assessment.

Set 3.12 Security Assessment

NORTHROP GRUMMAN

Which of the following NIST SP 800-171 controls are fully implemented in your organization? Please check all controls that have been fully implemented by your company.

- 3.12.1. Periodically assess the security controls in organizational 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 systems.
- 3.12.3. Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.
- 3.12.4. 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.

3.12.4 System Security Plan

NORTHROP GRUMMAN

Resource for Federal Systems (useful as a guide for your systems too):

- Guide for Developing Security Plans for Federal Information Systems
- NIST SP 800-18

3.12.2 Plan of Action and Milestones

NORTHROP GRUMMAN

Most Federal sites have Cyber Security Resources. Some useful materials are noted below and in the References section at the end of this training. These documents are from other problem domains, but relate to the same standard:

FedRAMP Plan of Action and Milestones (POA&M) Template

Centers for Medicare & Medicaid Services - Plan of Action and Milestones Process Guide

THE VALUE OF PERFORMANCE.

NORTHROP GRUMMAN

Certifications and Assessment Methodologies

Third Party Assessments of Security (Certifications)

NORTHROP GRUMMAN

The DoD and DFARS require self assessment.

- Making sure that your organization addresses all 110 controls with respect to CDI and Covered Contractor Information Systems.

- There is NOT a safe harbor third party assessment / certification that you can obtain.
  - Although some security firms may offer to do your self-assessment for you. (it is you who is ultimately responsible for compliance)

Industry Accepted Assessment Methodologies

NORTHROP GRUMMAN

There are industry accepted “certifications” for application of security best practices.

- Many apply to different industries, such as healthcare, financial services, etc.
- These are useful, but are not a replacement for your assessment against NIST SP 800-171.
- Examples: CMMI, ISO27001, many more

Capability Maturity Model Integration (CMMI)

NORTHROP GRUMMAN

> "The Capability Maturity Model Integration (CMMI)® is a globally-recognized set of best practices that enable organizations to improve performance, key capabilities, and critical business processes." – CMMI Institute Website

The Capability Maturity Model attempts to improve the assurance of a software product by assessing the vendors security engineering processes, rather than assessing the security of the product itself, which is a much more time consuming process.

- Third-party review of vendor security engineering processes (capabilities)
- Focus on measuring organization competency (maturity) and improvements
- Usually, this assessment is based on the application of industry and security best practices.

System Security Engineering Capability Maturity Model (SSE-CMM, ISO/IEC 21827)

NORTHROP GRUMMAN

- Two dimensions: *domain* and *capability*
- Domain is “base practices” of security engineering
  - E.g., Base Practice 05.02, “Identify System Security Vulnerabilities”
- Capability is “generic practices” that should be part of base practices
  - E.g., Generic Practice 2.1.1, “Allocate Resources”
- Intersection indicates an organization’s capability to perform a particular activity
  - E.g., “Does the organization allocate resources for use in identifying system security vulnerabilities?”

ISO/IEC 27000 family - Information security management systems

NORTHROP GRUMMAN

- The ISO/IEC 27000 family of standards helps organizations keep information assets secure.
- Using this family of standards will help your organization manage the security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties.
- ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS).
- -- source ISO Website

THE VALUE OF PERFORMANCE.
NORTHROP GRUMMAN

Useful References

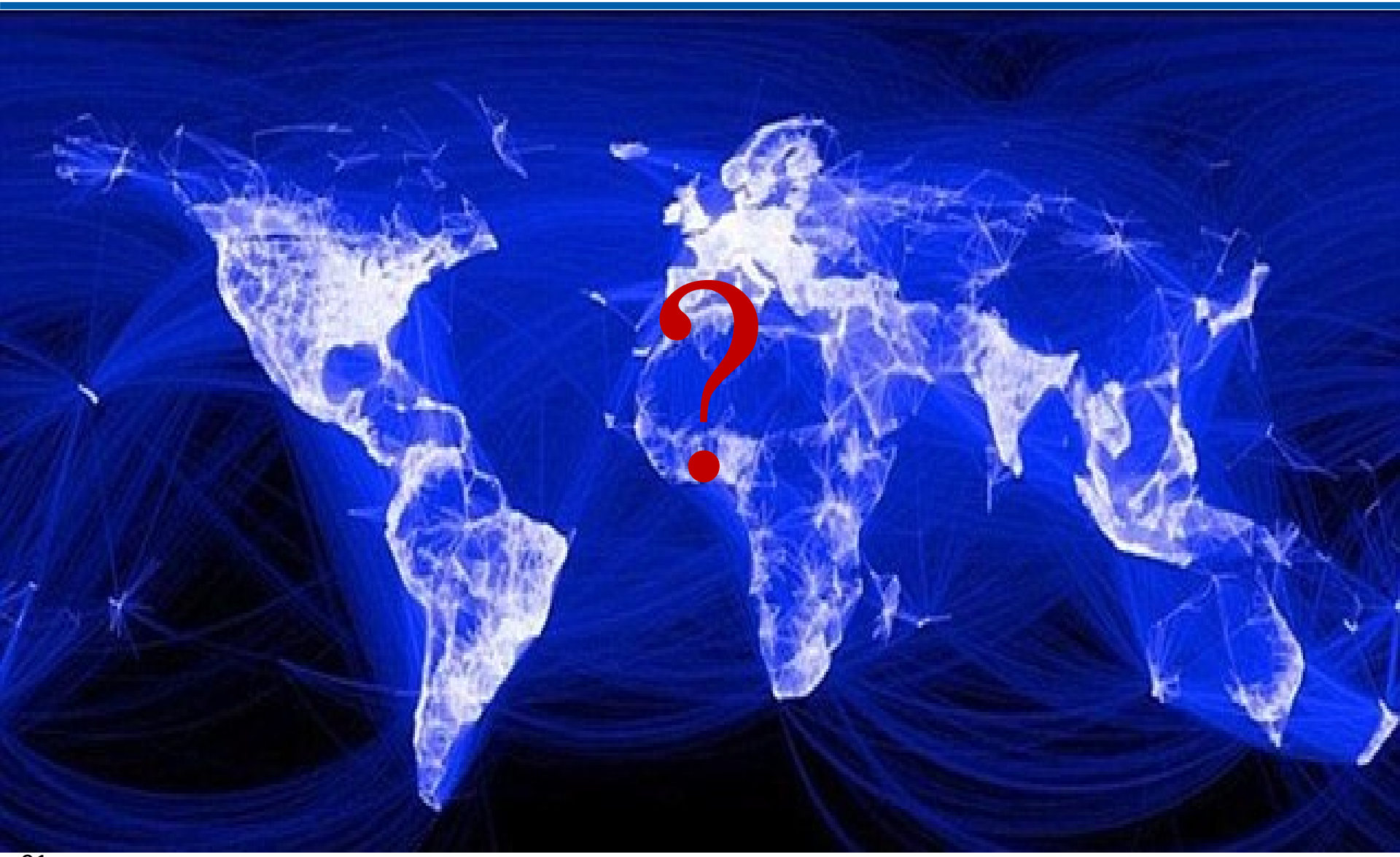
Useful References and Resources

NORTHROP GRUMMAN

- Cyber Security Resources for Suppliers
- Air Force Cyber Secure Website
- **NIST SP 800-171**
- Cyber Security Information for Small Business from various organizations:
  - https://www.dhs.gov/publication/stopthinkconnect-small-business-resources – Dept. of Homeland Security
  - https://www.sba.gov/managing-business/cybersecurity – Small Business Administration
  - https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business - Federal Trade Commission
  - www.fcc.gov/cyberplanner - FCC Small Biz Cyber Planner
  - www.NIST.gov/MEP/ NIST Manufacturing Extension Partnership

Questions

NORTHROP GRUMMAN



THE VALUE OF PERFORMANCE.

NORTHROP GRUMMAN