CYBERSECURITY
FOR GOVERNMENT CONTRACTORS:

(Can you prove your security posture?)

NDIA Forum
SMBs Cyber (and more)

15 May, 2015

Presented by:
Mike Davis
Mike.Davis.sd@gmail.com

with
Doug Magedman
Chris Simpson

www.ACMEcyber.com
Small Business Cybersecurity

Bottom Line Up Front (*BLUF*)

1. It's always all about enterprise risk management (ERM)
2. Long term authoritative source – cybersecurity framework
3. Reduce complexity – do the cyber basics well, encrypt!
4. You have TWO security environments, cloud and on site
5. Building in "Privacy by Design (PbD)" = continual compliance
6. Incident response plan (with cyber insurance and cyber counsel)
7. Affordable and defendable 'due diligence' security posture

When / If in doubt – go back to #1

Navigating the Cybersecurity Maze

A. What Are the Risk Areas?

B. Multiple parts / Random Motion

C. Requirements for Government Contractors

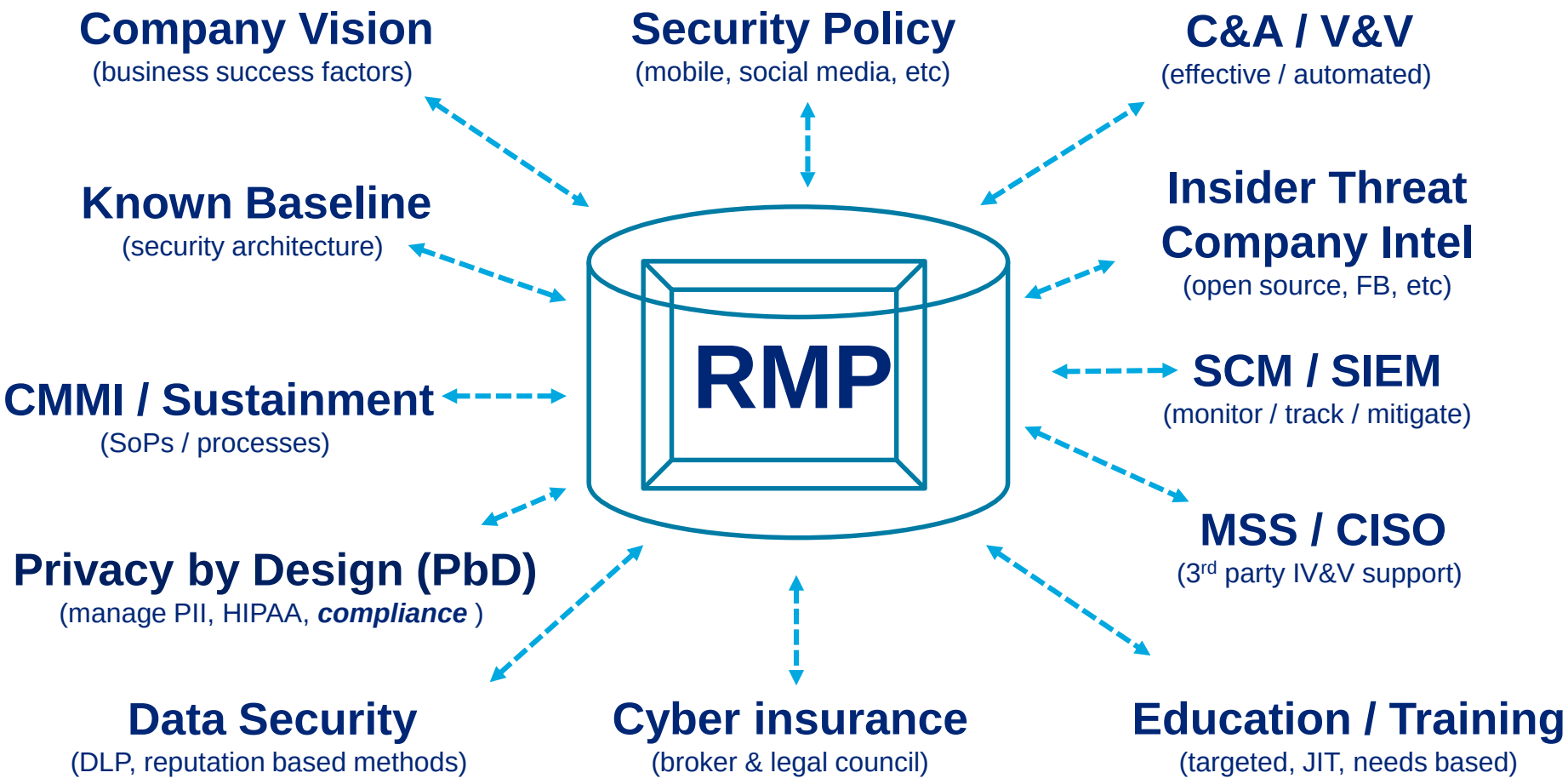
D. Expectations in 2015

E. NIST SP 800-171 overview and scope

F. Summary / recommendations

It's STIIL ALL ABOUT Enterprise RISK Management

+ Making privacy protection a full organizational contact sport +



Cyber must start with an *enterprise risk management plan* (RMP) / framework
AND use the NIST Cybersecurity Framework as the end-state / goal.

Data Breaches are expensive

Cost Of A Data Breach Jumps every year - *average cost of an attack is now $5.9M* *(Ponemon Study* – based on $200 / record *)

- More customers terminated their relationship with the company who had a breach
- Malicious or criminal attacks rather than negligence or system glitches were the main cause

Target, Home Depot, Chase.. Just the visible big ones

- National Archive and Records Administration, 2008: 76 million records
- Heartland Payment Systems, 2008-2009: 130 million records
- Sony online entertainment services, 2011: 102 million records
- Epsilon, 2011: 60 million to 250 million records
- Target, 2013: 110 million total records
- Home Depot, 2014: 56 million payment cards
- Target breach cost $200M to reissue cards and $100M to upgrade systems

There are two kinds of companies - those who've been hacked…and those who don't know they've been hacked." (*200 days, 3rd party*)

* Source: http://essextec.com/sites/default/files/2014%20Cost%20of%20Data%20Breach%20Study.PDF

Government Oversight Over The Intersection Of Its ITSystems And Its Private Contractors Is Mixed

- The titles of these GAO reports tell the story:
  - 2013 GAO Report, “Federal Information Security: Mixed Progress in Implementing Program Components; Improved Metrics Needed to Measure Effectiveness.”
  - 2014 GAO Report, “Information Security: Agencies Need to Improve Oversight of Contractor Controls.”

- No uniform cyber breach reporting requirements exist for government contractors.

- Agency coordination is improving, but gaps exist.
  - For example, an MOU between DoD and the FBI requires the FBI to inform DoD when it becomes aware of a cyber breach involving an Advanced Persistent Threat (“APT”) and a DoD contractor – but the FBI does not necessarily know who is a DoD contractor, much less who is an operationally critical contractor. DSS provides FBI with cleared contractors

Government specifics that follow, experts take from *Holland & Knight similar brief*

B – Multiple Parts / Random Motion

- "High-Risk Series: An Update," Report GAO-15-290 (Feb 2015), Over the past 8 years, the number of information security incidents reported by federal agencies to the U.S. Computer Emergency Readiness Team (US-CERT) has increased from 5,503 in fiscal year 2006 to *67,168 in fiscal year 2014, an increase of 1,121 percent..* http://www.gao.gov/products/GAO-15-290

What Are the Moving Pieces?

- Multiple agencies and players have overlapping roles.
- Different statutory and regulatory schemes also overlap.
- Congressional action and/or inaction has led to uncertainty.
- The Cyber Framework is 'voluntary'
- Even the cloud rules, FedRAMP, DISA "PA" et al are in motion

Who is in charge?

- Multiple agencies have overlapping roles:
  - The Federal Information Security Management Act ("FISMA") of 2002 gives OMB oversight of agency information security policies and practices, assigns NIST the role of developing security standards for agencies' computer systems (other than for national security systems), and requires each agency to adopt information system protections. The FISMA Modernization Act of 2014 expanded these roles.
  - The Cyber Executive Order assigns DHS an oversight role, which is codified by the FISMA Modernization Act.
  - Contracting agencies have their own cybersecurity requirements and clauses. **FAR 7.103(w) requires agencies to include FISMA compliance in their acquisition plans.**

Not Congress – catching up

- Congress has yet to act in a comprehensive way.
- The last major piece of cybersecurity law to be passed by Congress and was the E-Government Act of 2002, which included FISMA.
- Computer Security Act of 2012 came close to passage, but died in the Senate in August 2012. Issues were:
  - Opposition to industry-wide standards, even if voluntary.
  - Data privacy concerns.
  - Liability protections for compliant companies.
- To be fair, five discrete cybersecurity bills passed in 2014 and were signed by the President on December 19, 2014. These are:
  - **S1353: The Cybersecurity Enhancement Act of 2014**, which is unfunded and expressly states it does not create any regulatory authority. It amends the National Institute of Standards and Technology Act to require NIST to continue to support the development of voluntary standards for critical infrastructure (which NIST is already doing under the Framework). Requires a Cyber R&D Strategic Plan every 4 years.

2014 Cybersecurity Bills

-**S2519: The "National Cybersecurity Protection Act of 2014**." Amends the Homeland Security Act of 2002 to codify the existing Cybersecurity and Communications Integration Center, which promotes the sharing – on a voluntary basis – of information about cyber risks, incidents and analysis.

-**HR2952: The "Cybersecurity Workforce Assessment Act**." Requires DHS to conduct an annual analysis of the readiness and capability of its cybersecurity workforce and develop a "comprehensive" workforce strategy. Really.

-**S1691: The "Border Patrol Agent Pay Reform Act of 2014.**" Also amends the Homeland Security Act of 2002 to give DHS authority to establish excepted positions from the SES for cybersecurity-related functions in order to make it easier to hire cyber professionals.

-**S2521: The "Federal Information Security Modernization Act of 2014**." Codifies existing scheme of making OMB responsible for oversight of agency information security policies and practices, coordination with NIST to develop standards and guidelines, and oversee agency compliance. The Act requires the SecDef and DNI to perform these functions for DoD and IC national security systems, respectively. Each agency must submit an annual report to Congress, OMB and DHS detailing cyber breaches, and must perform an annual "independent" audit of its cybersecurity policies and practices. The audit must be performed by the agency Inspector General or by an outside auditor.

Congress inaction = Executive Order

The White House Executive Order 13636, 2013 “Improving Critical Infrastructure Cybersecurity”

Contains non-procurement-specific and procurement-specific elements. **The Framework will affect you one way or another:**

- Focuses on protecting cyber information according to identification of “critical infrastructure.”
- Directs NIST to develop a “Cybersecurity Framework” to reduce risks to critical infrastructure. The framework is to be technology-neutral and compliance with the resultant standards is to be voluntary.
- Agencies are to review the Framework and determine whether their existing cyber controls are sufficient and *whether their existing authority authorizes establishment of the requirements of the Cyber Framework on their regulated industries*.
- Expands current Enhanced Cybersecurity Services sharing program to owners and operators of critical infrastructure.
- The feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration.

NIST Cybersecurity Framework (CSF) Is *Voluntary*

- What does it do?
  "The Framework provides a common language for understanding, managing, and expressing cybersecurity risk both internally and externally. It can be used to help identify and prioritize actions for reducing cybersecurity risk, and it is a tool for aligning policy, business, and technological approaches to manage that risk. It can be used to manage cybersecurity risk across entire organizations or it can be focused on the delivery of critical services within an organization..

- How does it do it? (*re: around 100 IA controls*)
  - Framework **Core**: Identifies five activities – Identify, Protest, Detect, Respond, Recover – helpful to managing cyber risk.
  - Framework Implementation **Tiers**: These are categories of increasing cyber protection schemes against which an organization can measure itself. The tiers are: *Partial, Risk Informed, Repeatable, and Adaptive*.
  - Framework **Profile**: Companies can use the core and implementation tiers to prepare current profile and target profile, and develop an action plan to migrate from current profile to target profile.

- http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
- http://www.nist.gov/cyberframework/upload/nist-cybersecurity-framework-update-120514.pdf

CSF – Key points

- Who's covered?
  - Critical Infrastructure Sectors: Chemical; Commercial Facilities (i.e., sports arenas); Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Health Care and Health Services; Information Technology; Nuclear Reactors, Materials, and Waste; Transportation; and Water and Wastewater Systems.
  - Each sector has an agency lead; and a sector-specific plan since 2010.
  - Voluntary now, but Executive Order requires each agency to review the Framework and determine whether their existing cyber controls are sufficient and *whether their existing authority authorizes establishment of the requirements of the Cyber Framework on their regulated industries.*
  - At the very least, the Framework may be used as a "standard of care" in data breach cases. *(including the 'due diligence' execution aspects)*

"Improving Cybersecurity And Resilience Through Acquisition"

- DOD/GSA Joint Report (2014): Six recommendations:
  - **Institute baseline cybersecurity requirements as award conditions for appropriate acquisitions**.
  - Address cybersecurity in relevant training.
  - Develop common cybersecurity definitions for federal acquisitions.
  - Institute a federal acquisition cyber risk management strategy.
  - **Require purchases from OEMs, authorized resellers, or "trusted" sources**.
  - Increase government accountability for cyber risk management.

In addition, report states: "Cybersecurity standards used in acquisitions should *align to the greatest extent possible with international standards…."*

DFARS 204.73/Clause 252.204-7012: Safeguarding Unclassified Controlled Technical Information (*UCTI*)

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

- The rule applies to all new DoD solicitations, contracts, and newly modified existing contracts which involve UCTI)resident on, or transiting through, contractor unclassified information systems. The rule affects all DoD contractors and subcontractors, including vendors of commercial goods

- Contractors must use:
  - **NIST Special Publication 800-53**; or
  - If a NIST control is not implemented, the Contractor shall submit to the Contracting Officer a written explanation of how—
    - The required security control identified in the following table is not applicable; or
    - An alternative control or protective measure is used to achieve equivalent protection; or
  - Apply other information security requirements when the contractor reasonably determines that additional measures are needed based on an assessed risk.

DoD UCTI Rule (con’t)

Reporting requirement:

The Contractor shall report as much information as can be obtained within **72 hours** of discovery of any cyber incident, that affects unclassified controlled technical information resident on or transiting through the Contractor's unclassified information systems.

Damage Assessment:

- The contractor must conduct further review of its unclassified network for evidence of compromise resulting from a cyber incident to include, but is not limited to, identifying compromised computers, servers, specific data and users accounts. This includes analyzing information systems that were part of the compromise, as well as other information systems on the network that were accessed as a result of the compromise;
- Review the data accessed during the cyber incident to identify specific unclassified controlled technical information associated with DoD programs, systems or contracts, including military programs, systems and technology;
- Preserve and protect images of known affected information systems and all relevant monitoring/packet capture data for at least 90 days from the cyber incident to allow DoD to request information or decline interest;
- Support any DoD-conducted damage assessments, including providing system access and information.

DoD UCTI Rule (con't) – Technology challenges

1) Contractors must identify all of systems that *potentially* house or process UCTI.

2) Contractors must develop and implement system security controls for the applicable systems across 14 control vectors, as described in NIST SP 800-53

3) 3) System controls alone are insufficient to remain compliant with DFARS, and contractors require data controls to ensure the proper classification of data, proper protection of data access and use, and to provide sufficient logging of data use.. Yet, difficulty arises primarily, due to the vast and varied amounts of data in complex systems, there is a need for further clarification regarding what types of data specifically constitute UCTI

4) 4) Contractors need to develop automation that turns the application of solutions for DFARS compliance into efficiently repeatable, cost-effective processes. For example, to meet the 72 hour incident report timeline, as well as the damage assessment requirements, an automated process would be necessary to continuously capture all information that would be required by DoD in the event of a cyber incident.

DoD UCTI Rule (con't) – Business challenges

1) Contractors must develop new strategies and corporate policies in a timely manner in order to govern, and remain compliant with, DFARS requirements.

2) Contractors must develop a process to ensure that all newly created UCTI involved with a contract is identified, and appropriately labeled and controlled, as early as possible in its lifecycle

3) Contractors must also develop a process to properly identify and implement DFARS requirements for all legacy UCTI involved with new contracts or newly modified, existing contracts within their systems

4) Contractors face the task of training legal, compliance, engineering, operations, and IT departments in a complete set of new DFARS compliance processes

5) Contractors also face the challenge of vetting and/or managing all subcontractors in the supply chain to ensure they are compliant with DFARS

DoD Counterfeit Parts Rule

DoD May 2014 Rule: Detection and Avoidance of Counterfeit Electronic Parts

- Who is Covered?

  Contractors who are CAS covered – and their subcontractors regardless of CAS coverage –and that supply electronic parts or products that include electronic parts.

- What is a Counterfeit Electronic Part?

  An unlawful or unauthorized reproduction, substitution, or alteration that has been knowingly mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified electronic part from the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer. Unlawful or unauthorized substitution includes used electronic parts represented as new, or the false identification of grade, serial number, lot number, date code, or performance characteristics.

- Supply Chain Risk Management (**SCRM**) – a cyber black hole!

Other DoD Requirements

- NDAA 2013: Requires mandatory reporting of cyber breaches by cleared contractors.

- NDAA 2015: Requires the Secretary of Defense to establish procedures for mandatory reporting of cyber incidents experienced by "operationally critical contractors." This requirement was a result of the 2014 SASC Report referenced earlier.
  - Operationally critical contractors are those that are critical sources of supply for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.
  - DoD will designate and notify contractors falling within the definition of operationally critical contractors.
  - Rules due out in Q2 2015.

DoD Directive 5205.16, The DoD Insider Threat Program

- 2014, Unlike other DoD Directives, *it applies directly to contractors.*

- States that the Under Secretary of Defense for Acquisition, Technology, and Logistics is to develop contract clauses “to ensure DoD contracts impose uniform insider threat program requirements.”

- ALSO, Section 325 of the 2014 Intelligence Authorization Act requires the DNI to establish procedures requiring cleared IC contractors to report to the Government the successful penetration of a network or information system.

- The new procedures must create a mechanism for IC government personnel to obtain access to contractor equipment or information to enable the government to conduct its own forensic investigation.

I Don't Have DoD Contracts or Classified Work…. Am I Still Covered?

- In one word, "Yes." Remember **FISMA**?

  It seeks to set forth a framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets, including those operated by contractors.

  – **Each agency** must maintain an information security program that includes:
    - Periodic risk assessments;
    - Cost effective policies and procedures to address cybersecurity;
    - Subordinate plans for networks, facilities, and information systems;
    - Security awareness training;
    - Periodic testing and evaluation;
    - Remedial action where appropriate;
    - Procedures for detecting, reporting, and responding to security incidents;
    - Continuity plans.

  – ***Under FISMA, agencies can require contractors to meet these standards.***

What's Next for 2015?

2012 FAR *Proposal To* Regulate Cybersecurity: *What Happened To It?*

- Government information may not be processed on computers without access control or located in public areas.
- Electronic information may be transmitted only on systems that utilize technologies and processes that provide the **best level of security** and privacy available, given facilities, conditions and threat level.
- Transmission by voice or fax may only occur when the sender has a reasonable assurance that access is limited to authorized recipients.
- Systems must be protected by at least one level of physical barrier and one level of electronic barrier, such as lock and key in conjunction with a password, when not in the direct control of the individual user.
- Media that is being released or discarded must be cleared and sanitized.
- The contractor must provide at least the following means of intrusion protection: Current and regularly updated malware protection, such as anti-virus software and anti-spyware software; and prompt application of security-related upgrades and patches.
- Information may only be transferred to those subcontractors with a contractual need to have the information and who employ the safeguards described in the clause.

Summary: What Applies To Government Contractors Now?

- DFARS UCTI Rule, which references NIST 800-53.
- DOD Counterfeit Electronic Parts rule.
- NDAA 2013 mandatory reporting (no regs yet).
- 2014 Intelligence Authorization Act (no regs yet).
- NDAA 2015 Requirements for Operationally Critical Contractors (no regs yet).
- Current FAR / DFAR
- Individual Agency Regulations and Clauses.
- Soon companies that process or access classified information may have to establish insider threat programs
  - The Defense Security Service is expected to amend the National Industrial Security Program Operating Manual (NISPOM)

Other required standard processes

- Compliance Program Basics
- Assessing Risks And Requirements
- Written Policies
- Training
- Capable Official In Charge
- Periodically Review And Assess Your Program
- Use incentives and Consequences
- Tone From The Top (*and the Middle)
- Report, Track, And Resolve Incidents
- Addressing Cybersecurity In Your Agreements
- Employment Agreements And Policies
- Legal Instrument/Terms To Consider

Expanded details and recommendations for each in back-up.

Common Issues For Small Businesses

- Nascent IT systems -- are your employees still using gmail for business purposes? Are non-employees using your email domain?
- Reliance on part-time help and BD consultants.
- Work may be disbursed geographically -- how do you maintain physical security?
- Who owns the server(s) your data resides on?
- Leverage (or lack of it) with contracting partners.
- ACCESS, ACCESS, ACCESS…
- Contractual Obligations… Legal Requirements
- Insider Threats Are Possibly The Greatest Risk Area
  - What remedies do you have in place?
  - How will you document and prove your case?
  - When do your problems become reportable to the Government?

November 2014 NIST SP 800-171 Draft

- "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations."

- Part of overall government effort to streamline classification and handling of controlled unclassified information ("CUI"), which is information subject to restrictions on dissemination, such as export controlled-information, FOUO, or technical data:
  - The National Archives and Record Administration ("NARA") has promulgated regulations (pending before OMB) to streamline and make uniform the government categories of protected, unclassified information.
  - The November NIST draft contains standards which government contractors who handle CUI must meet.
  - The FAR will be amended to incorporate the NIST standards, once finalized.
  - Companies will want to review the standards included in the NIST draft to measure against their current policies and procedures.

We decompose the SP 800-171 and map to the cyber suite functions

NISTR 800-171 Summary

EO 13556 – CUI (Nov 2010) – directed action, NARA as Executive Agent

The bigger picture:

- Federal CUI rule (32 CFR part 2002) – requires controls and markings
- NIST SP 800 – 171, define security requirements, based on FIPS 200 and NIST SP 800-53
- DFAR 204.73 to apply Federal CUI rule and SP 800-171 to contractors
- When CUI is in nonfederal IS / organizations, protecting *confidentially of data*

800-171 SECURITY REQUIREMENT - *14 FAMILIES*

FAMILY	FAMILY
Access Control	Media Protection
Awareness and Training	Personnel Security
Audit and Accountability	Physical Protection
Configuration Management	Risk Assessment
Identification and Authentication	Security Assessment
Incident Response	System and Communications Protection
Maintenance	System and Information Integrity

Addresses the “4 P’s” (people, process, policy and product)

CUI Registry:
http://www.archives.gov/cui/registry/category-list.html
UCTI / 171 overview brief (confidentiality impact is no lower than “*moderate*” iaw FIPS 199()
http://www.isaca-washdc.org/presentations/2015/201504_session4.pdf

MUST do IA Controls *(# direct / derived (**CUI**) / assumed (**NFO**))*

1. **ACCESS CONTROL** (**2 / 20 & 5**) : Limit information system access to authorized users.

2.**AWARENESS AND TRAINING** (**2 / 1 & 2**): Ensure that managers and users of organizational information systems are made aware of the security risks and ensure that personnel are adequately trained.

3.**AUDIT AND ACCOUNTABILITY** (**2 / 7 & 4**) : Create information system audit records to enable the reporting of unlawful, unauthorized, or inappropriate information system activity; and ensure that the actions of individual users can be traced and held accountable for them.

4.**CONFIGURATION MANAGEMENT** (**2 / 7 & 10**) : Establish baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation); and establish security configuration settings for technology products.
(note - *add in contingency planning* (**1 / 21**) (back-up))

5.**IDENTIFICATION AND AUTHENTICATION** (**2 / 9 & 2**) : Identify information system users and authenticate (or verify) the identities of those users as a prerequisite to allowing access.

6.**INCIDENT RESPONSE** (**2 / 1 & 6**) : Establish an operational incident-handling capability for organizational information systems; and track, document, and report incidents to authorities.

7.**MAINTENANCE** (**6 / 3**) : Perform periodic maintenance on organizational information systems; and provide effective controls on the tools and personnel used for maintenance.

MUST do IA Controls (cont) (**133** / **116**)

8. **MEDIA PROTECTION** (**3 / 6 & 1**) : Protect information system media containing CUI, both paper and digital; and limit access to CUI on information media to authorized users.

10. **PHYSICAL PROTECTION** (**2 / 4 & 13**) : Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

9.**PERSONNEL SECURITY** (**3 / 4**) : Screen individuals prior to authorizing access to information systems containing CUI.

11.**RISK ASSESSMENT** (**1 / 3 & 3**) : Periodically assess the risk to organizational operations, assets, and individuals. (note – *add in PLANNING* (**0 / 6**)

12.**SECURITY ASSESSMENT** (**3 / 6**) : Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; develop and implement plans of action designed to correct deficiencies.

(note - add in *systems / service acquisition controls* (**1 / 13**) (ISSE)

13.**SYSTEM AND COMMUNICATIONS PROTECTION** (**2 / 14 & 8**) : Monitor, control, and protect organizational communications (i.e., information transmitted or received by information systems).

14.**SYSTEM AND INFORMATION INTEGRITY** (**3 / 4 & 15**) : Identify, report, and correct information and IS / IT flaws in a timely manner; and provide malicious code protection.

Sample set of ALL IA controls required (*CM*).

NIST SP 800-53 MODERATE BASELINE SECURITY CONTROLS		TAILORING ACTION
CM-1	Configuration Management Policy and Procedures	NFO
CM-2	Baseline Configuration	CUI
CM-2(1)	*BASELINE CONFIGURATION | REVIEWS AND UPDATES*	NFO
CM-2(3)	*BASELINE CONFIGURATION | RETENTION OF PREVIOUS CONFIGURATIONS*	NCO
CM-2(7)	*BASELINE CONFIGURATION | CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS*	NFO
CM-3	Configuration Change Control	CUI
CM-3(2)	*CONFIGURATION CHANGE CONTROL | TEST / VALIDATE / DOCUMENT CHANGES*	NFO
CM-4	Security Impact Analysis	CUI
CM-5	Access Restrictions for Change	CUI
CM-6	Configuration Settings	CUI
CM-7	Least Functionality	CUI
CM-7(1)	*LEAST FUNCTIONALITY | PERIODIC REVIEW*	CUI
CM-7(2)	*LEAST FUNCTIONALITY | PREVENT PROGRAM EXECUTION*	CUI
CM-7(4)(5)	*LEAST FUNCTIONALITY | UNAUTHORIZED OR AUTHORIZED SOFTWARE / BLACKLISTING OR WHITELISTING*	CUI
CM-8	Information System Component Inventory	CUI
CM-8(1)	*INFORMATION SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATIONS / REMOVALS*	NFO
CM-8(3)	*INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION*	NCO
CM-8(5)	*INFORMATION SYSTEM COMPONENT INVENTORY | NO DUPLICATE ACCOUNTING OF COMPONENTS*	NFO
CM-9	Configuration Management Plan	NFO
CM-10	Software Usage Restrictions	NCO
CM-11	User-Installed Software	CUI

Security Questions from a PRIME *(6 of 28)*

1. Does your company --have cyber security policies, procedures, and standards based on industry standards (e.g. ISO 27000, NIST 800-53), and require they be used to manage all IT devices and/or services (i.e. e-mail, data storage, web pages, etc) that process and/or store sensitive information received from a third-party company?
2. Protect sensitive information received from a third-party company during transmission between the owning third-party as well as other parties with whom that data is shared (i.e. Encryption, SSL/TLS connections)?
3. Are all devices that store or process a third-party company's sensitive information protected from the Internet by a firewall?
4. A dedicated, full-time employee or subcontracted IT staff?
5. A dedicated, full-time employee or subcontracted cyber security staff?
6. A cyber security user education and awareness program?

What are the measures, thresholds – *what is good enough = YES*?

Security Questions from a PRIME *(6 more of 28)*

7. Perform cyber security audits by objective internal employees or external 3rd parties on IT systems/devices and IT services that store or process sensitive information at least annually?

8. Do all devices that store or process sensitive information at a minimum have commercially available antivirus with current signature files?

9. Do all devices that store or process sensitive information at a minimum have a unique user name and complex password to access the system?

10. Do all devices that store or process sensitive information at a minimum have access control that is configured on a least privilege model (a person only has access to the data/device that they need)?

11. Do all devices that store or process sensitive information at a minimum have vulnerability scanning performed at least monthly AND are vulnerabilities being remediated in a risk based priority (highest priority vulnerabilities are fixed first)?

12. Do all devices that store or process sensitive information at a minimum have all unnecessary ports and services disabled and the device is used for limited functions (ex. A device acting solely as a file server vs. a file server, FTP server, and web server)?

What are the measures, thresholds – *what is good enough = YES*?

Security Questions from a PRIME *(7 more of 28)*

13. Do all devices that store or process sensitive information at a minimum have patches deployed for high risk operating system and third-party application vulnerabilities within industry best practices (i.e. 48 hours) and medium/low risk patches to be deployed in <= 30 days?

14. Are all laptop devices that store sensitive information encrypted?

15. Do all mobile devices (e.g. smartphones, tablets) that store sensitive information at a minimum have configuration management provided by a company owned centrally managed infrastructure?

16. Do all mobile devices (e.g. smartphones, tablets) that store sensitive information at a minimum have access control to the device (complex password to access device)?

17. Do all mobile devices (e.g. smartphones, tablets) that store sensitive information at a minimum have the ability to remotely wipe the device?

18. Does your company have a Computer Incident Response Team (CIRT) with a formal process to respond to cyber attacks?

19. When your company must share sensitive information, does your company require those suppliers to follow policies, and procedures for cyber security based on industry standards (e.g. ISO 27000, NIST 800-53)?

What are the measures, thresholds – *what is good enough = YES*?

Security Questions from a PRIME *(9 more of 28)*

20. Require 2-factor authentication for remote access (e.g. token used in addition to a username and password for VPN login)?
21. Perform industry standard (e.g. ISO 27000, NIST 800-53) logging and monitoring on devices that store or process sensitive information?
22. Control web access based on the risk (e.g. reputation, content, and security) of the sites being visited (e.g. Web Proxy Controls)?
23. Capabilities of detecting and blocking malicious e-mail prior to delivery to the end user?
24. Tools and processes to mitigate Advanced Persistent Threats (APT)?
25. Perform full packet capture?
26. Actively participate in a cyber intel sharing forum? (e.g. ISAC, Infraguard, Local FBI, US-CERT, etc)?
27. Perform phishing e-mail testing of its employees?
28. A team (employee or subcontracted) that is capable of performing forensics in support of investigations?

What are the measures, thresholds – *what is good enough = YES*?

General industry common practices

1) **Harden Systems** –first implement system security controls and strengthen their systems' security. To implement system controls that are compliant with DFARS, contractors must ensure the appropriate system controls are implemented on all of their systems that store or transit UCTI.

2) **Define Policies** – After hardened systems, DFARS compliant policies should be developed to govern access to UCTI. In order to define polices that will govern access to this data, contractors should implement corporate policies and training programs to govern the DFARS process.

3) **Classify Data** – Next, develop policies to identify where their UCTI resides, and what classifications will be applied to what types of data. In order for contractors to properly classify data according to DFARS, they must develop detailed knowledge about the UCTI that must be protected.

4) **Enforce Controls** – Once UCTI is identified, contractors must put system and data controls in place across all of their systems where UCTI may reside to govern the access and use of UCTI to ensure only authorized users may access and download data.

5) **Automated Tracking** – In order to remain compliant with DFARS requirements mandating contractors to provide access logs within 72 hours of a cyber incident, contractors should implement automated log collection to record all access to UCTI on their systems. And also to support a forensic analysis that can quickly assess the extent of potential damage following a cyber incident.

OMG – How can anyone sort that all out?

Step back a bit – clarify the fog of cyber security – ERM!

IF you use AND maintain the *standard 'cyber suite'*

- Address the people, process, policy and products aspects (SMB cyber safe)
- Implement the general industry best security practices, include mobile / telework
- And DO the cyber security basics well – follow the CISO fundamentals
- ***You will 'naturally' address the 171 controls*** *AND* show 'due diligence'

The CSF will be "*THE*' reference to map to (*think CMMI*)

The **100** or so "CIP" controls map to the **133**+ in "DoD" in 800-171

Map the 800-171 IA controls into a checklist (Appendix E)

YOU will need PROVE each IA control (which are based on 800-53)

Side benefits - consider applying under the SAFETY ACT
(DHS: covers services, products, policies, etc) (re: *minimizes tort liability*)

Summary / Key take-aways

- KNOW your baseline, HW, SW, SoPs, etc…
- Practice, monitor & enforce cyber hygiene.
- Strictly control access – especially privileged accounts.
- Encrypt – monitor & track data too (DLP / DRM)
- Comprehensive monitoring (SCM / SIEM)
- Proactive Privacy monitoring / audit = continual compliance.
- Use open systems intelligence (OSI) to know YOUR threats
- Enterprise risk management approach
- Cyber SME / MSSP – reach back tech support
- Cyber insurance & Cyber Savvy Legal counsel

Cyber Safe* goes well beyond DoD rules, *it's good business

The Purpose Of Compliance Programs

- The primary focus of any compliance program is to prevent and detect misconduct or breaches – cyber security is no different
- Secondary purposes include:
  - To ensure compliance with contractual obligations
  - To mitigate or avoid monetary damages/consequences
  - To preserve reputation
  - To mitigate or avoid other sanctions or suspension and debarment

Government specifics that follow, experts take from *Holland & Knight similar brief*

Compliance Program Basics

- Sound compliance programs consist of important common features:
  - Written codes of conduct/procedures tailored to the company's circumstances
  - Regular training for employees
  - A senior official of the company being charged with responsibility
  - Periodic monitoring of the program
  - Discipline for violations
  - Compliance as a key to advancement
  - Demonstrated commitment by Management
  - Appropriate reporting and issue resolution policies
- Each of these is relevant to addressing cybersecurity compliance.

Remember Compliance Program Basics

- Sound compliance programs consist of important common features:
  - Written codes of conduct/procedures tailored to the company's circumstances
  - Regular training for employees
  - A senior official of the company being charged with responsibility
  - Periodic monitoring of the program
  - Discipline for violations
  - Compliance as a key to advancement
  - Demonstrated commitment by Management
  - Appropriate reporting and issue resolution policies
- Each of these is relevant to addressing cybersecurity compliance.

Assessing Risks And Requirements

- Before you can develop written policies or training materials, you have to assess risks and legal requirements:
  - Review your contracts
  - Review relevant government regulations and policies
  - Review industry standards and best practices
  - Review your organization's experience with cyber security
  - Review your organization's systems, structure and existing compliance measures
  - Consider related, existing compliance policies
- See Part I for examples of where to look: NIST 800-171 identifies the areas to be included in a cyber assurance policy.

Written Policies

- Depending on agency requirements, Cybersecurity should either be integrated into your existing property, data and records management policies or in a separate policy.
- Consider whether property, data and records management policies are consistent with your cybersecurity requirements.
- Disseminate revised policies when ready.

Training

- Use the content of your revised written policies to guide training content.
- Make sure training is provided on a regular basis, that participation is meaningful and tracked, and that you document your efforts.
- Make sure content and methods of delivery are effective and geared toward the audience.

Put A Capable Official In Charge

- The person needs to have real authority and the respect of peers;
- The person needs to be knowledgeable and have access to updates in the field;
- The person needs to have resources to carry out their role (including sufficient time in their own day); and
- The position needs to be incorporated into the reporting hierarchy of your organization.

Review And Assess Your Program Regularly

- Regular review (annually at least) is essential.
- Be prepared to adjust or enhance your program based on any of the following:
  - Changes in your company's characteristics (i.e., growth, new product lines, new locations, etc.)
  - Changes in your customers requirements (i.e., changes to contracts, policies, etc.)
  - Experience, including breaches, patterns of activity and so on
  - Changes in law or policy
- Document your reviews and your program/policy changes.

Make Sure There Are Consequences

- Violations must result in Consequences.
- Positive actions should be rewarded.
- Particularly if you are in a highly regulated area, consider making this part of
  - Employee reviews
  - Hiring decisions

Tone From The Top (*and the Middle)

- Management should set a good example in…
  - Their day-to-day behavior
  - Participating in training and other compliance activities
  - Their messaging to employees and the outside world
- Don’t’ forget middle management
  - Employees interact with them more often in most cases
  - They are essential in maintaining compliance and your culture of compliance

Report, Track, And Resolve Incidents

- Detecting potential issues is essential.
- Make sure employees know where to go in the event of a breach.
- Make sure the party receiving the reports is equipped to handle them properly and knows whether further reporting is required.
- Document all response efforts even if the conclusion is no breach occurred or no action is needed.
- Periodically review data in a macro sense to identify risks, trends and needs for enhancement to your program.
- Consider providing summary reports to upper management to track your experience.

B. Addressing Cybersecurity In Your Agreements

- Consider cyber requirements in contract performance:
  - Subcontracts
  - JV agreements
  - Teaming Agreements
- Try to lead in the “battle of the forms”
  - To ensure you understand requirements
  - Requirements meet your capabilities/systems
  - To avoid inconsistent obligations

Employment Agreements And Policies

- Consider cyber in your employment agreements, especially for positions related to contracts covered by enhanced requirements.
- Consider cyber in your employee handbooks (make sure good cyber practices are a basis for continued employment).
- Consider cyber issues in your hiring decisions and in your diligence.
- Consider the extent to which you should monitor employee behavior (i.e., tracking emails, system access, social media, etc.).

Third Party Agreements

- Consider cyber in your other third party agreements, such as:
  - Business Development support
  - PEOs and Temp agencies
  - Professional services providers (accountants, lawyers, etc.)
  - IT support (i.e., data storage and “The Cloud”)

Legal Instrument/Terms To Consider

- What legal instruments/terms and conditions might help?
  - NDAs
  - Non-competes
  - Employee handbooks and compliance program materials
- Restrictive legends on key documents and within certain systems
  - i.e., drafts of proposals
  - Underlying cost and pricing data
  - Other proprietary and confidential information