Cybersecurity Compliance: Requirements & Options

DFARS 204.73
DFARS 239.76
FAR 4.19
NIST (SP) 800-53 & 800-171

Michael G. Semmens
Imprimis, Inc.
June 2017

AGENDA

- The Nature of Cyber Threats
- Compliance Requirements
- Approaches and Available Resources
- Summary

The Nature of Cyber Threats

Threats by Domain

Defense Requirements

The Two Sides of Cyber

Productive Applications
via the Cyber Domain

Threats
via the Cyber Domain

Productive Applications

Productive Applications
via the Cyber Domain

- Advanced Manufacturing
- Smart Grid – Smart Energy
- Digital Healthcare
- Transportation
- Space
- … and Many, Many More

In Cyber Shangri-La, the full potential of technology on global GDP is realized as cyber security one-ups the bad guys for a net global gain of $190 trillion. The worst-case scenario, where the bad guys win - Clockwork Orange Internet - drains $90 trillion of potential net economic benefit from global GDP." [By 2030] [Zurich Insurance Group]

ZURICH

Cyber Threats

Threats
via the Cyber Domain

The loss of industrial information and intellectual property through cyber espionage constitutes the "greatest transfer of wealth in history,"

[General Keith Alexander, NSA Director 2012]

Has Anyone Heard of a Cyber Incident Lately?

Doug Olenick, "**Cyber Enemies"**, *SCMagazine*, May 2017: 15-17. Print.

Top 3 Chinese Hacks

1. OPM – Office of Personnel Management
2. FDIC
3. Various Industrial Espionage

Top 3 Russian Hacks

1. 2016 Presidential Election
2. Democratic National Committee
3. Yahoo!

Hey, wait a minute – that ain't nothing – how about …

- **The F-35**
- **Technology Targeting**

- **Estonia 2007**
- **Georgia 2008**
- **Ukraine &**
- **Ukraine Power 2015**
- **(BTW – no one hacked the election)**

Top 3 North Korean Hacks

1. Sony Entertainment
2. SWIFT
3. Interpark

Top 3 Criminal Hacks

1. Home Depot
2. Anthem 2015
3. Mirai (Dyn 2016)

Top 3 Terrorist Hacks

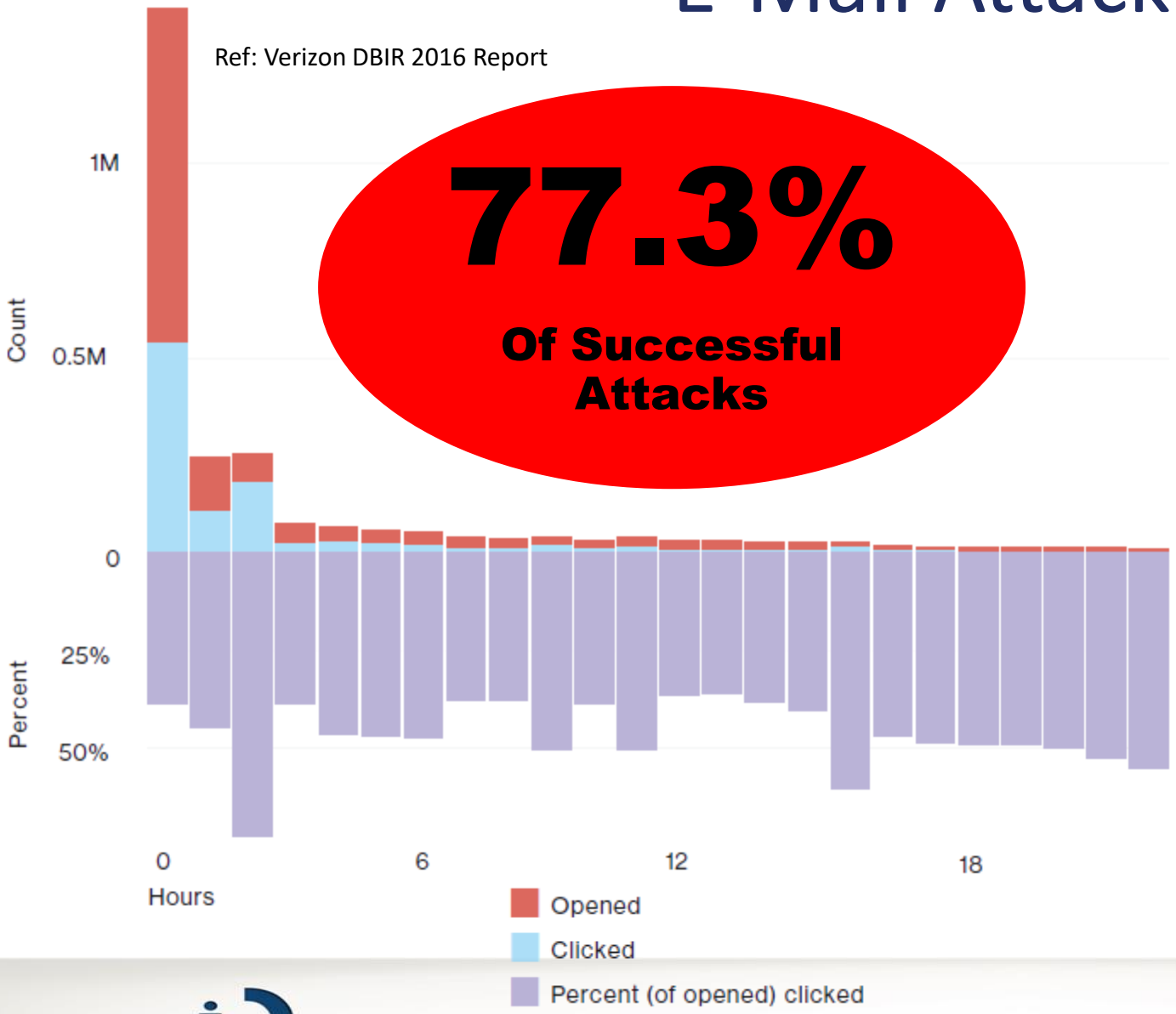
1. CENTCOM Twitter
2. Newsweek Twitter
3. Islamic State Hacking of Division's (ISHD) Kill List (a.k.a., Cyber Caliphate, Islamic Cyber Army or ICA)

Cyber Threat Players and Activities

	APT (Advanced Persistent Threat)	CYBER CRIME	HACKTAVIST	INSIDER THREAT	TERRORIST	NUISANCE
ACTORS	Nation States, Major Crime Org's	Amateurs to Nations	Amateurs to Major Org's	Authorized User / Admin.	Individual, Non-State, Nation State	Unskilled or Less Able Actors
OBJECTIVE	Espionage, Dis-Enable, Destroy, Defeat	Theft of Valued Data	Discredit, Disrupt, Cause Havoc	Sensitive Information, Revenge, Profit	Disrupt, Destroy, Kill	Financial, Recognition
TTP: TECHNIQUES TACTICS PROCEDURES	Social Eng., Phishing, Advanced TTPs, Implant 'Low & Slow'	Social Eng., Phishing, Escalate Privileges, Exfil. Data	Social Eng., Phishing, DOS/DDOS (Distributed Denial of Service)	Use Authorized Access to Steal, Sabotage, Damage	Social Eng. To Advanced TTP	SPAM, Scanning, Crawlers, Worms, Viruses
MAJOR KNOWN SOURCES	China, Russia, Iran, North Korea	Russia, China, "Riders of the Dark Net"	Political, Ethnical, Religious Org's or Individuals	Throughout	North Korea, Al Qaeda, ISIS /ISIL, … many	Ubiquitous

E-Mail Attack Vector

Ref: Verizon DBIR 2016 Report



Number of phishing emails opened and clicked in first 24 hours and percent of opened emails that were clicked

Email Phishing

A form of social engineering in which a message, typically an email, with a malicious attachment or link is sent to a victim with the intent of tricking the recipient to open an attachment or following a link

IMPRIMIS INC

Why Should All Companies Care?

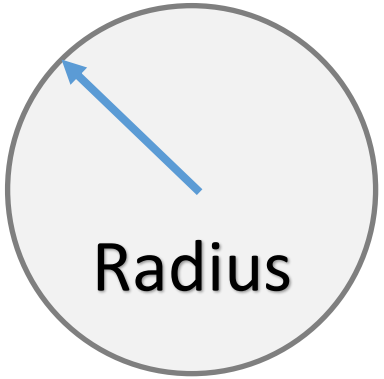
- *"Hey, I'm just a small business. No one cares enough about what we do to bother with a cyber attack. What would they get?"*

- PII (Personally Identifiable Information)
- PHI (Protected Health Information)
- IP (Intellectual Property)
- Money
- Spectrum of Sensitive Information, and …
- Your Cyber Vector Radius™ (CVR™)

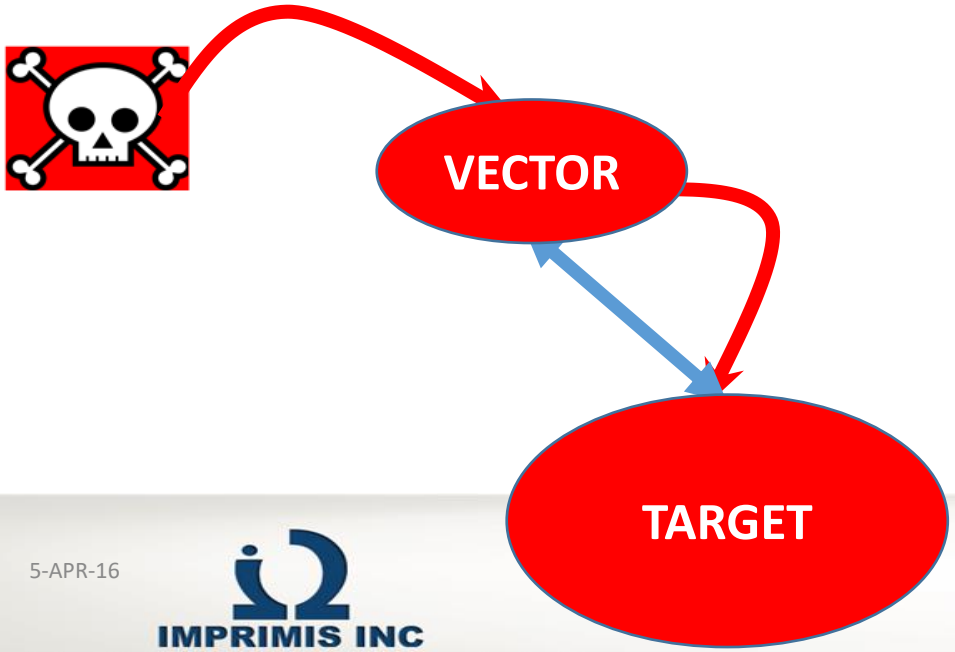
About Your Vector Radius

VECTOR: In physics and geometry, a vector is used to represent physical quantities that have both magnitude and direction

RADIUS: A straight line from the center to the circumference



ATTACK VECTOR: the particular approach used, or vulnerability exploited, in order to penetrate a computer system's security or propagate malicious software



- There are no PHYSICAL dimensions in cyberspace – a computer in Beijing or Moscow is as close to you as your officemate's computer.
- The concepts of space and separation are gone.
- The (attackers) are bad guys in your offices and your homes.

SUMMARY

- The quality of life and the economic performance of the US and the world can be greatly enhanced by the appropriate application of cyber related technology
- The ubiquitous nature of cyber technology combined with the open culture of our “cyber community” present such a huge vulnerability to enemies and criminals alike that it could – if unchecked – diminish the US in the extreme

Best Practices & Recommendations

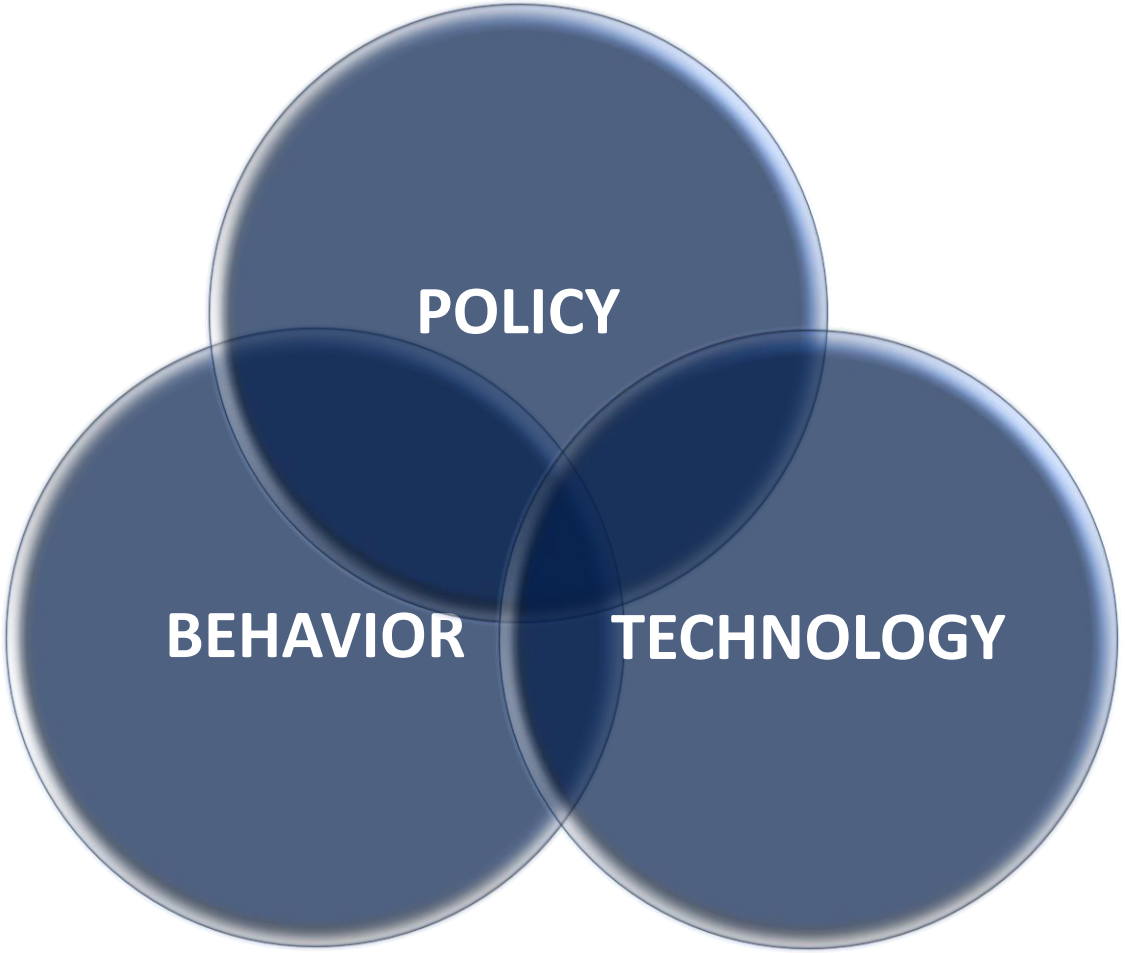
Executive Responsibility

- Cybersecurity and Compliance programs are needed within a Corporation for the purpose of…
  - ❖Managing Risk and Liabilities
  - ❖Meeting Minimum Requirements to Access Markets
  - ❖Achieving and Maintaining Competitive Advantage

Cybersecurity is a Fiduciary Responsibility of the Organization's

- **Board of Directors,**
- **Officers,**
- **Senior Leadership and Management**

Components of Cybersecurity



The Smart Cyber Citizen™

- Protect Credentials
  - Password (Complexity & Change_)
  - Password Manager
  - Do not use important passwords in public places
- Protect Hardware
  - Firewall
  - Antivirus / End Point Protection
  - Patching & Updating
- Protect Data
  - Classify Data
  - Backup (on & off line)
  - Encrypt key data when & if you can
  - Basic physical security

USE WHAT YOU KNOW TO STAY SAFE:

1. Do not accept e-mails from people you do not know
2. Do not download an attachment or click a link unless you are ABSOLUTELY CERTAIN it from or to a safe source
3. If you receive an odd e-mail from someone you do know – verify it with them – watch out for Cyber Posers
4. If you delete an important e-mail it can be re-sent with little effort– if you respond to a bad e-mail data or money is gone forever – and your job may be too!

The Cyber Big 10 For Organizations

- Control Access
- Control Configuration: Inventory & Control Devices and Programs
- Segment Networks
- Classify Data & Encrypt Liberally
- Develop a Cybersecurity Architecture That Employs Both Strong Perimeter & Active (Defenses in Depth)
  - Firewall, Anti-Virus, Intrusion Detection/Prevention
- Scan Periodically – Scan Regularly
- Train & Test ALL Staff, and then Train Them Again
- Develop, Implement, Train, Test and Exercise Your
  - Incident Response Plan
  - Business Continuity Plan (**All Backups**)
- Improve Each and All Areas Continuously
- Be a Member of an Organization(s) That Can Provide Cyber Threat Intelligence, Alerts, Exercises, Training, and Resources

Best Practices Lead to Standards

- The Big 10 look a lot like the security families in NIST 800-171
- Cyber Standards are the consensus best practices for cybersecurity
- Adopting a standard is a best practice for any organization
- The best thing for an organization to do is get started – you will find it is not that hard and the benefits are significant

- … Besides, if you do contract work for the U.S. Government you are going to have to comply with NIST 800-171 or stop working for the USG

DFARS

(Defense Federal Acquisition Regulation Supplement)

204.73 (subpart) **Safeguarding Covered Defense Information and Cyber Incident Reporting**

- 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting
- 252.204-7008 Compliance with Safeguarding Covered Defense Information Controls
- 252.204-7009 Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information

202.1 (subpart) **Definitions**

239.76 (subpart) **Cloud Computing**

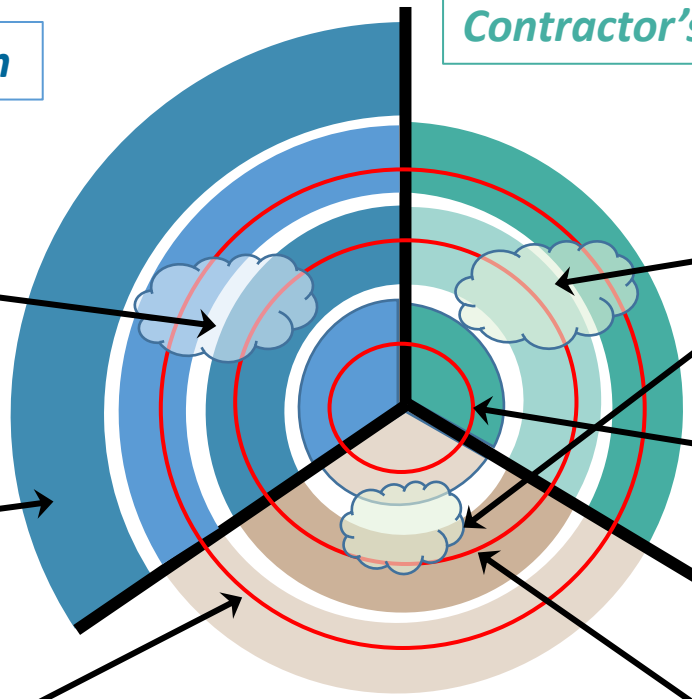
- 252.239-7009 Representation of Use of Cloud Computing
- 252.239-7010 Cloud Computing Services

212.301 (f) (clauses & provisions) **Solicitation provisions and contract clauses for the acquisition of commercial items**

Government Presentation (DPAP)

Navigating Unclassified Cyber/Information (System) Security Protections

Elements that drive appropriate protections. The information system and the information



Contractor's Internal System

Applicable controls:
NIST SP 800-171

Cloud Service Provider (CSP)

Applicable controls:
FedRAMP (Mod)

Contractor's System Operated on DoD's Behalf

Applicable controls:
From CNSSI 1253, based on NIST SP 800-53

Cloud Service Provider (CSP)

Federal Contract Information

Unclassified Controlled Technical Information (UCTI)

Controlled Unclassified Information (CUI) (USG-wide)

DoD Information System

Applicable controls:
From CNSSI 1253, based on NIST SP 800-53

Covered Defense Information (CDI)

DFARS

SUBPART / CLAUSE	TITLE	REQUIREMENTS
204.73 (subpart)	**Safeguarding Covered Defense Information and Cyber Incident Reporting.** *Revised – Oct 21, 2016*	▪ Contractors & Subcontractors must safeguard 'Covered' defense information that resides in or transits through contractor 'UNCLASSIFIED' information system. ▪ For Contractor Systems, FedRAMP qualified cloud providers will be used ▪ Must rapidly report incidents involving possible loss of covered data to DoD via Dibnet.dod.mil ▪ Report will include i) incident report, ii) malicious software, and iii) media ▪ Prescribes: 252.204-7008, -7009, -7012 , 252.227-7013
202.1 (subpart)	**Definitions.** *Revised - Oct 21, 2016*	▪ Designated subpart as location for definitions:
239.76 (subpart)	**Cloud Computing.** *New Addition – Aug 26, 2015* *Revised - Oct 21, 2016*	▪ For Federal Systems, contracts will be awarded to cloud service providers that are granted provisional authorization by DISA using DISA SRG. ▪ Prescribes 252.239-7009 & -7010
212.301 (f) (clauses & provisions)	**Solicitation provisions and contract clauses for the acquisition of commercial items.** *Revised – August 2, 2016*	▪ Identifies Solicitation clauses and provisions to be included in the acquisition of commercial items. ▪ Includes cybersecurity and safeguards identified in the above clauses. ▪ Supply chain risk evaluation required (239.73)

D F A R S

SUBPART / CLAUSE	TITLE	REQUIREMENTS
204.73 (subpart)	**Safeguarding Covered Defense Information and Cyber Incident Reporting.** *Revised – Oct 21, 2016*	▪ Contractors & Subcontractors must safeguard 'Covered' defense information that resides in /through contractor 'UNCLASSIFIED' information system. ▪ Must rapidly report incidents … to DoD via www.dibnet.dod.mi ▪ Report will include i) incident report, ii) malicious software, and iii) media ▪ Prescribes: 252.204-7008, -7009, -7012
252.204-7012 (clause)	**Safeguarding Covered Defense Information and Cyber Incident Reporting.** *Revised – Sept 21, 2015* *Revise - Dec 30, 2015* *Revised Oct 21, 2016*	***(a) Definitions. [Please see Table of Definitions]*** ***(b) Adequate security.*** ▪ Contractor will implement information systems security protections on all covered contractor 'UNCLASSIFIED' information systems ▪ If operated on **behalf of the Government** – for Cloud follow **DFARS 252.239-7010**, ▪ Contractor (Offeror) **represents that it will implement security requirements in NIST 800-171 as soon as practical but no later than December 31, 2017** ▪ For all contracts awarded **prior to October 1, 2017**, the contractor shall **notify the DoD Chief Information Officer (CIO)**, via email at osd.dibcsia@mail.mil within **30 days** of contract award ▪ Contractor will **apply other information system security measures** when the contractor reasonably determines that additional security measures are required. ▪ "Alternative but equal effective" security measures … submitted in writing to an "authorized representative of the DoD CIO," who will "adjudicate" offeror requests. ▪ If Contractor intends to use an **external cloud service provider** … security requirements … for the **Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline** ***(c) Cyber incident reporting requirement.*** ▪ Contractor will **rapidly report incidents within 72 hours** to … prime contractor and DoD via http://dibnet.dod.mil ▪ Medium Assurance Certificate required

DFARS

SUBPART / CLAUSE	TITLE	REQUIREMENTS
204.73 (subpart)	**Safeguarding Covered Defense Information and Cyber Incident Reporting.** *Revised – Oct 21, 2016 Continued*	
252.204-7012 (Continued)	**Safeguarding Covered Defense Information and Cyber Incident Reporting.** *Revised – Sept 21, 2015* *Revise - Dec 30, 2015*	*(d) Malicious software.* ▪ When Contractor discover and **isolate malicious software** submit the malicious software to **DoD Cyber Crime Center (DC3)**-not the Contracting Officer. *(e) Media preservation & protection.* ▪ When a cyber incident has occurred, the Contractor shall **preserve and protect images** of all known affected information systems and all relevant monitoring/packet capture data for at **least 90 days** *(f) Access to additional information or equipment necessary for forensic analysis.* ▪ Upon request, Contractor will **provide access to additional data and equipment for forensics** *(g) Cyber incident damage assessment activities.* ▪ If requested, Contractor will **provide all damage assessment information.** *(h) – (k) DoD safeguarding and use of contractor attributional/proprietary information.* *(l) Other safeguarding or reporting requirements.* ▪ The safeguarding and cyber incident reporting required by this clause in no way abrogates the Contractor's responsibility for other safeguarding *(m) Subcontracts.* ▪ Contractor will **include this clause on any subcontracts**, or similar contractual instruments, for which subcontractor performance will involve covered defense information … including reporting. ▪ The Contractor shall— **Require subcontractors** to— (i) **Notify the prime Contractor** (or next higher-tier subcontractor) when submitting a **request to vary from a NIST SP 800-171**; and (ii) Provide the **incident report number**, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable, **when reporting a cyber incident to DoD** as required in paragraph (c) of this clause.

DFARS

SUBPART / CLAUSE	TITLE	REQUIREMENTS
204.73 (subpart)	**Safeguarding Covered Defense Information and Cyber Incident Reporting.** *Revised – Sept 21, 2015*	▪ Contractors & Subcontractors must safeguard '***Covered***' defense information that resides in or transits through contractor (IT) system. ▪ Must submit to DoD i) incident report, ii) malicious software, and iii) media. ▪ Prescribes: 252.204-7008, -7009, -7012
252.204-7008 (provision)	**Compliance with Safeguarding Covered Defense Information Controls.** *New Addition - Aug 26, 2015* *Revised - Dec 30, 2015*	▪ **All contractors represent to implement NIST 800-171 as soon as practical, but no later than December 31, 2017**, or ▪ Contractor must **notify the DoD Chief Information Officer (CIO),** within 30 days of award, of ANY NIST SP 800-171 **security requirement that has NOT been implemented** at the time of contract award.
252.204-7009 (clause)	**Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.** *New Addition – Aug 26, 2015* *Revised - Dec 30, 2015*	▪ Contractor agrees to use contractor or 3rd party information for supporting government activities and no other use. ▪ A 3rd party reporting an incident is a 3rd party beneficiary to the Non-disclosure agreement between the Contractor and the government. ▪ Contractor shall include this clause, including this paragraph (c), in subcontracts, or similar contractual instruments, for services that include support for the Government's activities related to safeguarding covered defense information and cyber incident reporting, including subcontracts for commercial items, without alteration, except to identify the parties

DFARS

SUBPART / CLAUSE	TITLE	REQUIREMENTS
239.76 (subpart)	**Cloud Computing.** *New Addition – Aug 26, 2015*	▪ DoD will acquire cloud computing using commercial T&Cs consistent with Federal Law. ▪ Contracts will be awarded to cloud service providers that are granted provisional authorization by DISA. ▪ Prescribes 252.239-7009 & -7010
252.239-7009 (provision)	**Representation of Use of Cloud Computing.** *New Addition – Aug 26, 2015*	▪ The **Contractor will be required to provide**, as a part of its offer, a **Representation of Intent to use Cloud Computing Services** in performance of the contract.
252.239-7010 (clause)	**Cloud Computing Services.** *New Addition – Aug 26, 2015*	▪ **Representation at time of offer** or **written approval** by the contracting officer required **before using cloud computing**. ▪ Safeguards and controls to be implemented in accordance with **DISA Cloud Computing Security Requirements Guide (SRG)** ▪ Use of data for contract purposes only ▪ Incident reporting to http://dibnet.dod.mil ▪ Notification of 3rd party request for data ▪ Subcontractor Flow-Down required

FAR

(Federal Acquisition Regulation)

Subpart 4.19 Basic Safeguarding of Covered Contractor Information Systems

52.204-21 Basic Safeguarding of Covered Contractor Information Systems

NARA REQUIRES CUI IN 2016

NARA, CUI Requirements, and the FAR Clause

Executive Order 13556, Controlled Unclassified Information, November 4, 2010, established the CUI Program and designated the National Archives and Record Administration (NARA) as its Executive Agent to implement the Order and to oversee agency actions to ensure compliance with the Order.

Regarding contractors, the CUI Executive Agent anticipates establishing a single Federal Acquisition Regulation (FAR) clause in 2016 to apply the requirements of NIST Special Publication 800-171 to the contractor environment as well as to determine oversight responsibilities and requirements. The CUI Executive Agent also addresses its oversight of federal agencies in the proposed regulation for incorporation into the Code of Federal Regulations. Approaches to oversight will be determined through the uniform CUI FAR clause, future understandings, and any agreements between federal agencies and their nonfederal information-sharing partners.

--Special Publication NIST 800-171, page 15.

The FAR 15/NIST 800-171 Differences

Any Federal Acquisition will FAR 52.204-21.

There are 15 FAR requirements that essentially are NIST 800-171 requirements with 2 exceptions:

FAR 52.204-21 Specified Requirements	Corresponding NIST (SP) 800-171 Requirements
(vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.	3.8.3 Sanitize or destroy information system media containing CUI before disposal or release for reuse.
(ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.	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.

CUI Registry (https://www.archives.gov/cui/registry/category-list)

FINAL NOTE

- Some aerospace prime contractors including Lockheed, BAE Systems, Boeing, Raytheon, and Rolls-Royce have agreed to use the cloud based solutions of EXOSTAR LLC to comply with the cyber DFARS.
- They employ two (2) 'check the box' questionnaires; one based on the Center for Internet Security (CIS) Top 20 Critical Security Controls (CSC) – commonly referred to as the SANS 20, and the other based on NIST 800-171
- They require a signed representation of 'truthful statements'
- They claim they prefer a "risk management approach" rather than a "compliance" approach
- Exostar is privately held owned by Lockheed Martin, BAE Systems, Boeing, and Raytheon.

The Contractor is responsible for complying with NIST 800-171 and it should be well documented.

- The contractor signs the 'Certs & Reps' in each proposal submitted
- Soon the contractor will be required to submit the SSP & POA&M
- The contractor records will be examined by the government in the event of an incident
- No other standards or guidelines satisfy this requirement
- Only the government can approve alternative security controls within NIST 800-171

Besides, the questionnaires are much easier to complete if you have done your assessment and compliance first!

NIST 800-171

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

NIST 800-171

NIST 800-171 Security Families	
AC - Access Control (3.1)	22
AT - Awareness & Training (3.2)	3
AU - Audit & Accountability (3.3)	9
CM - Configuration Management (3.4)	9
IA - Identification & Authentication (3.5)	11
IR - Incident Response (3.6)	3
MA - Maintenance (3.7)	6
MP - Media Protection (3.8)	9
PS - Personnel Security (3.9)	2
PE - Physical Protection (3.10)	6
RA - Risk Assessment (3.11)	3
CA - Security Assessment (3.12)	3 /4
SC - System & Communications Protection (3.13)	16
SI - System & Information Integrity (3.14)	7
TOTAL REQUIREMENTS:	109 110

REV 1 – NIST 800-171 (Is Final)

- Guidance on the use of system **security plans (SSPs)** and **plans of action and milestones (POAMs)** to demonstrate the implementation or planned implementation of CUI requirements by nonfederal organizations;
- **Guidance on federal agency use of submitted SSPs and POAMs** as critical inputs to risk management decisions and decisions on whether or not to pursue agreements or contracts with nonfederal organizations;

3.12.4 Develop, document, periodically update, and implement **system security plans** for organizational information systems that describe the security requirements in place or planned for the systems.

System Security Plan or SSP:

1. System Definition
2. Governance
3. Risk Assessment / Categorization
4. Compliance Assessment + Remediation Plan (POA&M)

NIST 800-171… NOW HAS 110 REQUIREMENTS

NIST 800-171 TAILORING

- The Government started with the FIPS Moderate Baseline
- They removed controls that …
  - Pertained only to the government (FED)
  - Did not support "C" or Confidentiality (NCO)
  - Expected to be routinely satisfied by the non-federal organization (NFO)

TAILORING SYMBOL	TAILORING CRITERIA
NCO	NOT DIRECTLY RELATED TO PROTECTING THE CONFIDENTIALITY OF CUI.
FED	UNIQUELY FEDERAL, PRIMARILY THE RESPONSIBILITY OF THE FEDERAL GOVERNMENT.
NFO	EXPECTED TO BE ROUTINELY SATISFIED BY NONFEDERAL ORGANIZATIONS WITHOUT SPECIFICATION.
CUI	THE CUI BASIC OR DERIVED SECURITY REQUIREMENT IS REFLECTED IN AND IS TRACEABLE TO THE SECURITY CONTROL, CONTROL ENHANCEMENT, OR SPECIFIC ELEMENTS OF THE CONTROL/ENHANCEMENT.

APPENDIX E: NIST SPECIAL PUBLICATION 800-171

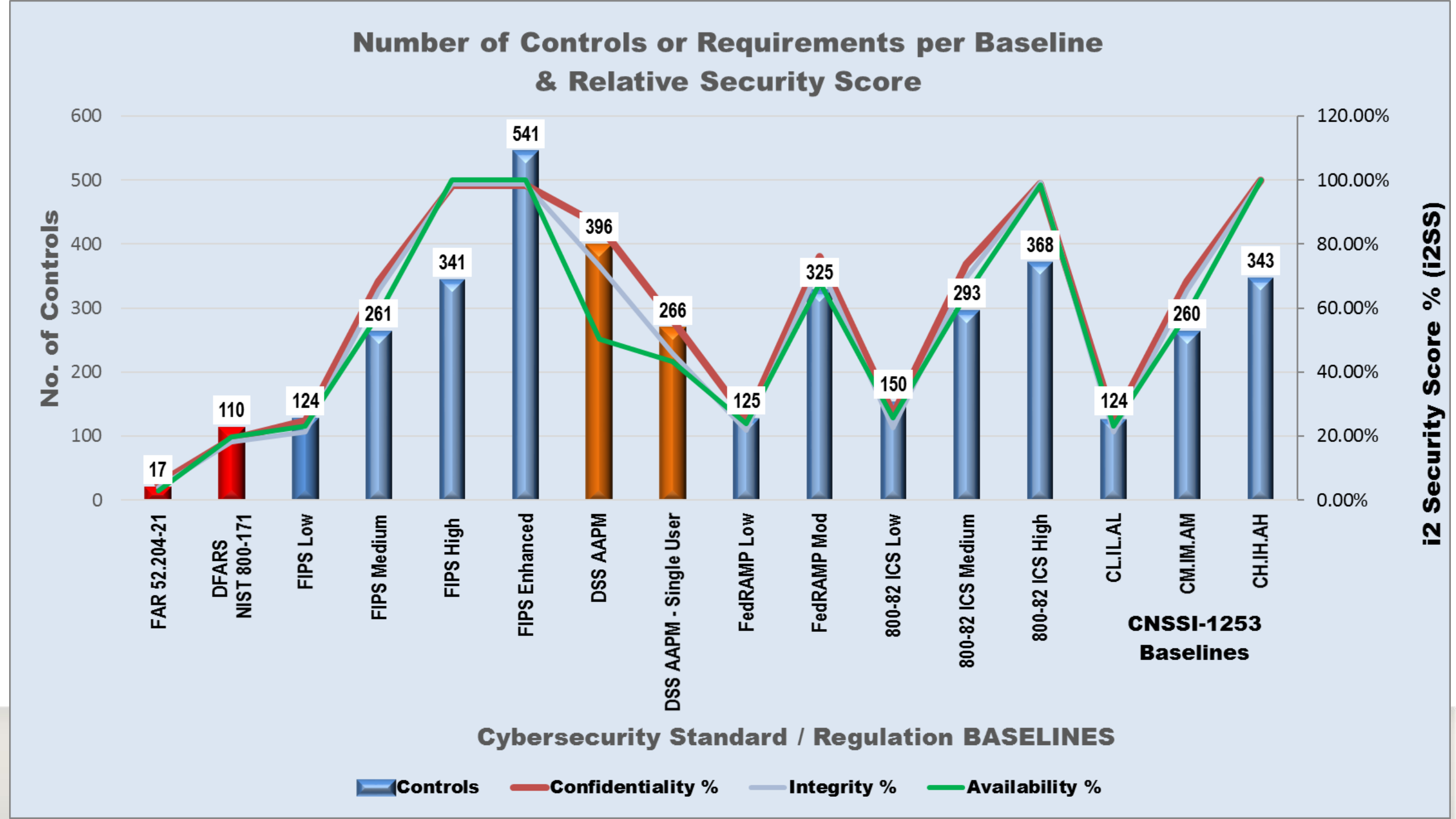
When To Use NIST 800-171

- NIST 800-171 is intended for use by federal agencies with recommended requirements for protecting the *confidentiality* of **Controlled Unclassified Information (**CUI) :
  - when the CUI is resident in **nonfederal information systems** and organizations;
  - where the CUI does not have specific safeguarding requirements prescribed by the authorizing law, regulation, or government wide policy for the CUI category or subcategory listed in the **CUI Registry** (https://www.archives.gov/cui/registry/category-list); and
  - when the information systems where the CUI resides are *not* operated by organizations on behalf of the federal government.
- The requirements apply *only* to components of nonfederal information systems that process, store, or transmit CUI, or provide security protection for such components
- Federal agencies will include CUI requirements in appropriate contractual vehicles established between those agencies and nonfederal organizations
- Nonfederal organizations must comply with these requirements to meet contractual requirements

More Requirements?

- DFARS 252.204-7012
  - Contractor (Offeror) **represents** that it will **implement security requirements** in **NIST 800-171 as soon as practical but no later than December 31, 2017**.
  - Contractor **will apply other information system security measures** when the contractor reasonably determines that [additional] security measures are required.
- There are 65 NFO controls from about all security families
- The Implementation Guides at DPAP make it clear that breaches and incidences will be investigated and the contractor will cooperate
- A solid plan with a rationale that can be defended is needed

Do What is Right … and Do It Right!

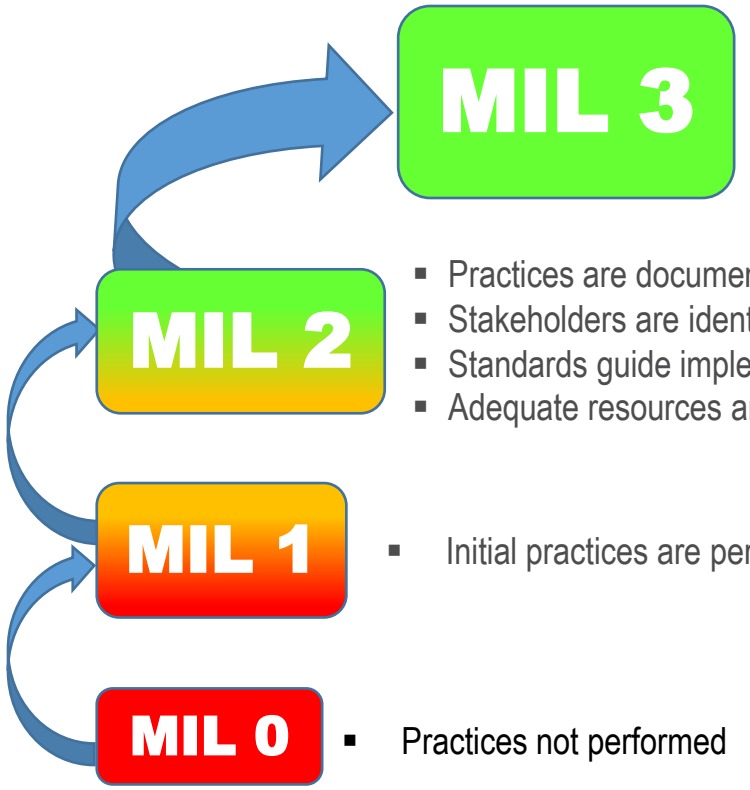

Number of Controls or Requirements per Baseline
& Relative Security Score
No. of Controls
i2 Security Score % (i2SS)
600
500
400
300
200
100
0
120.00%
100.00%
80.00%
60.00%
40.00%
20.00%
0.00%
17
110
124
261
341
541
396
266
125
325
150
293
368
124
260
343
FAR 52.204-21
DFARS NIST 800-171
FIPS Low
FIPS Medium
FIPS High
FIPS Enhanced
DSS AAPM
DSS AAPM - Single User
FedRAMP Low
FedRAMP Mod
800-82 ICS Low
800-82 ICS Medium
800-82 ICS High
CL.IL.AL
CM.IM.AM
CH.IH.AH
CNSSI-1253 Baselines
Cybersecurity Standard / Regulation BASELINES
Controls
Confidentiality %
Integrity %
Availability %

Cybersecurity Maturity Model

CMMI Maturity Levels		
LEVEL	TITLE	CHARACTERISTICS
5	**Optimizing**	Focused on continuous process improvement
4	**Quantitatively Managed**	Process measured and controlled
3	**Defined**	Process is described & proactive
2	**Managed**	Process is described but reactive
1	**Initial**	Process not/ poorly described, reactive

Capability Maturity Model Integration (CMMI) Institute, a subsidiary of ISACA (originally Information Systems Audit and Control Association)

Maturity Indicator Level (MIL) Characteristics



- **MIL 3**
  - Activities are guided by policy and governance
  - Policies include compliance to specified standards
  - Responsibility and authority are assigned
  - Personnel have adequate skills and knowledge
- **MIL 2**
  - Practices are documented
  - Stakeholders are identified and involved
  - Standards guide implementation
  - Adequate resources are provided
- **MIL 1**
  - Initial practices are performed but ad hoc
- **MIL 0**
  - Practices not performed

Cybersecurity Capability Maturity Model Version 1.1
DoE/DHS February 2014

OPTIONS

Resources

- DHS, NIST, GOVERNMENT
- DIB ISAC (Defense Industrial Base, Information Sharing & Analysis Center)
- The i2 Cyber Compliance Center (C3 or the Cube)

Tools

- Spreadsheet
- CSET (Cyber Security Evaluation Tool)
- i2ACT-800

ISACs & ISAOs

DIB
DEFENSE INDUSTRIAL BASE
CRITICAL INFRASTRUCTURE PROTECTION
INFORMATION SHARING AND ANALYSIS CENTER

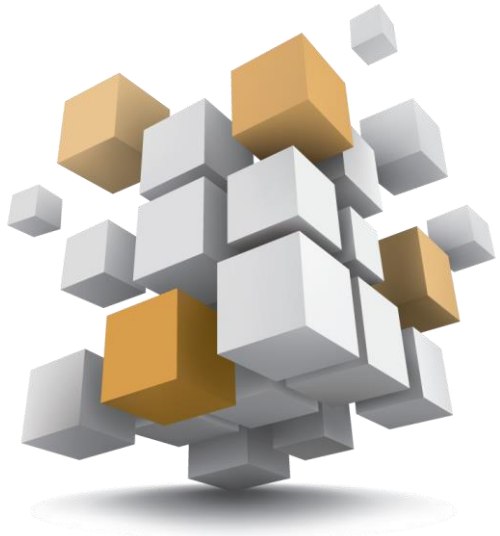
Cyber Verify™ is the DIB ISAC process for Verifying and Certifying Compliance

The DIB ISAC selected the Imprimis Compliance Tool

- National Infrastructure Protection Plan (NIPP) called for Information Sharing & Analysis Centers (ISAC) in each industrial sector (total 21)
- DoD established the DIB Cyber Security (DIB CS) Program for cleared defense contractors:
  - Operates DIBNet
- DHS is also establishing Information Sharing & Analysis Organizations (ISAO)

I2 Cyber Compliance Center: C3 or 'The Cube'

A Center in Colorado Springs Providing Compliance Support Nationally



- **SERVICES**
  - System Definition
  - Compliance Assessment
  - Vulnerability Assessment
  - Remediation Support
  - Blue Team Preparation
  - Support Through Read Team Audit
- **FACILITIES & RESOURCES**
  - VTC/Telephonic/Remote Access
  - Training & How-to Videos
  - Policy & Plans Templates
  - Vulnerability Scanning Tools
  - Penetration Testing
  - Monitoring Services /Tools
  - Support During Incident Response

CONTACT INFORMATION

719.785.0393

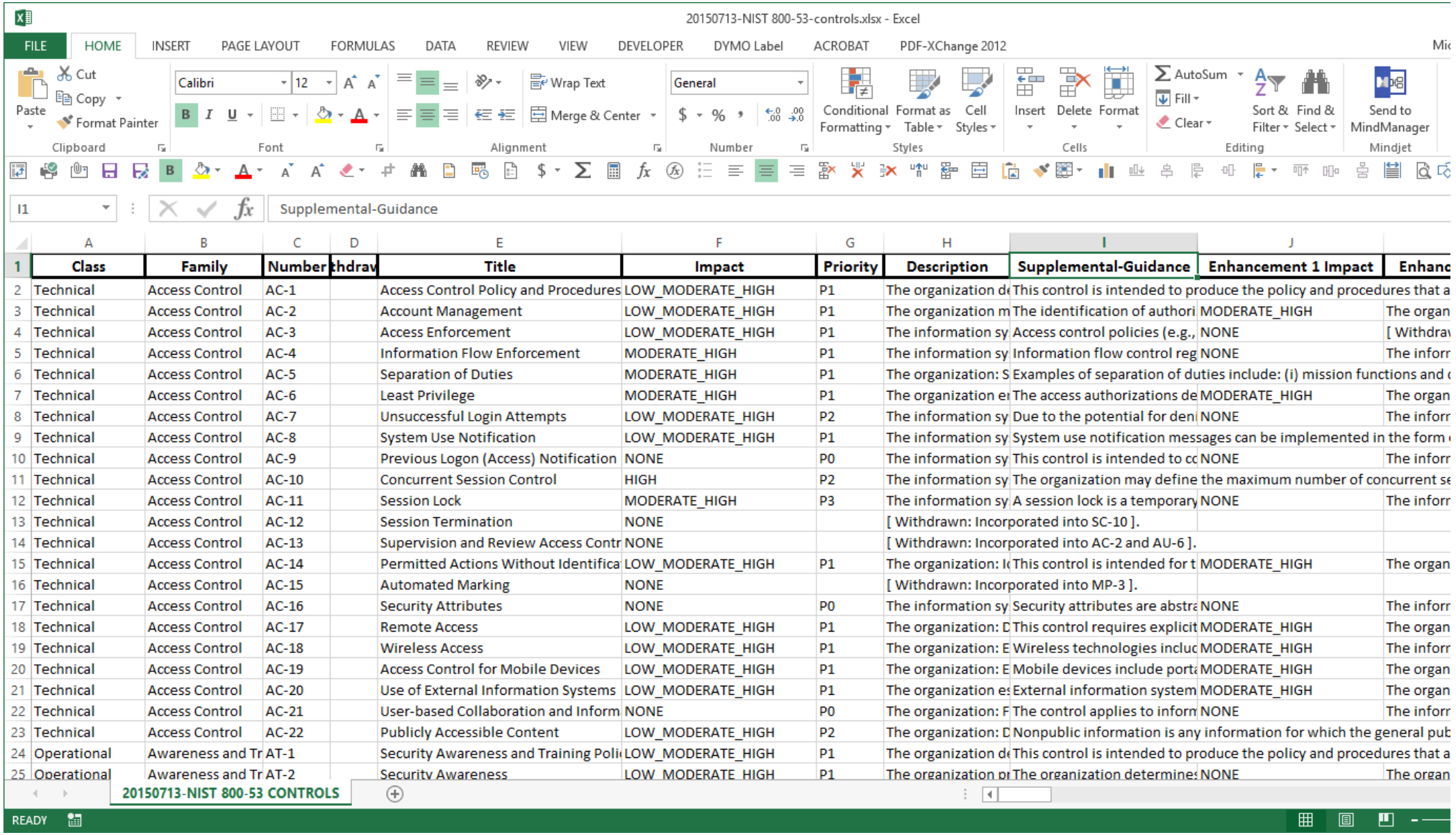
info@i2standards.com

www.i2compliancetools.com

(Support)

Option #1

Spreadsheet
With Word & file-sharing

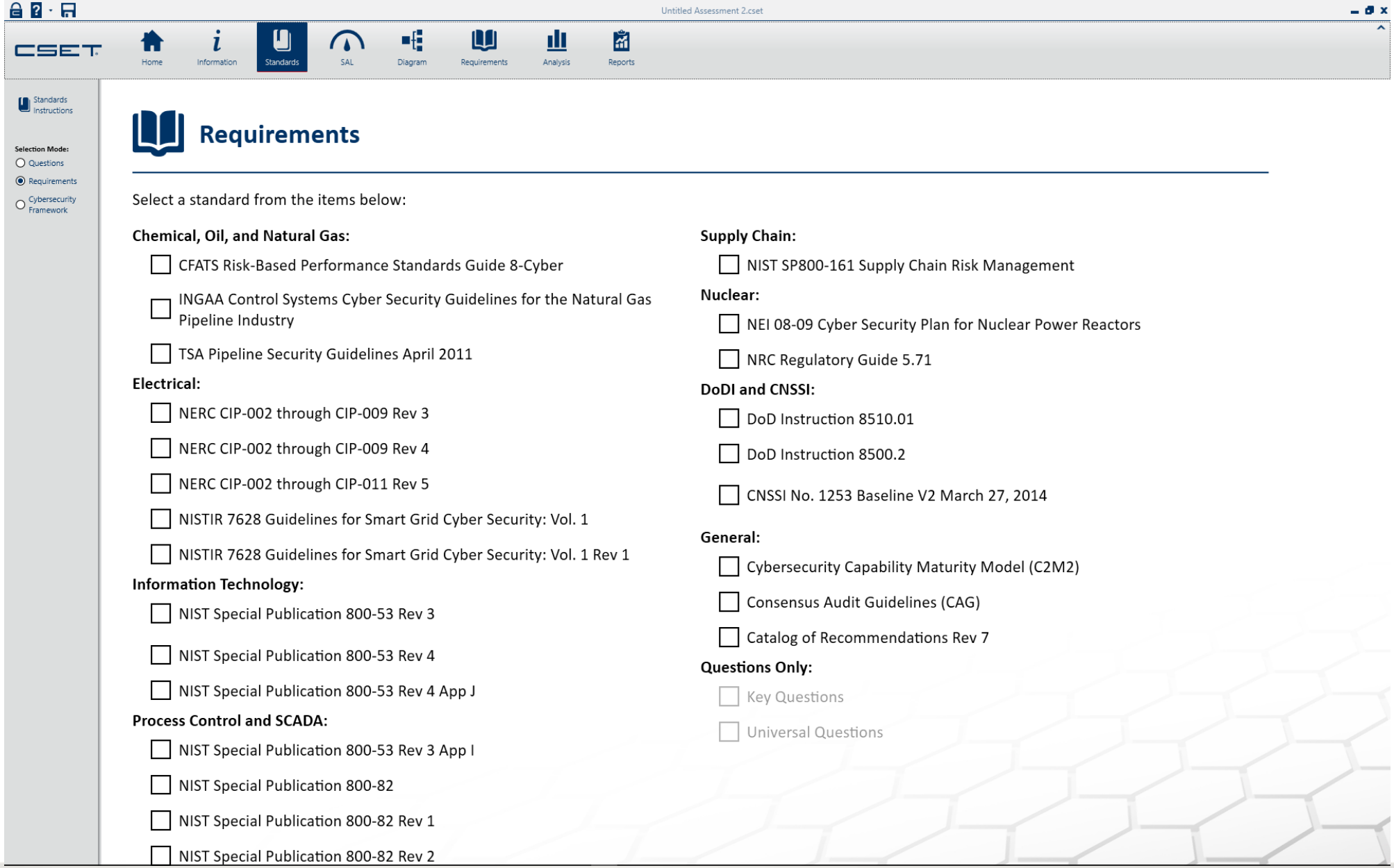


Class	Family	Number	Withdrawn	Title	Impact	Priority	Description	Supplemental-Guidance	Enhancement 1 Impact	Enhanc
Technical	Access Control	AC-1		Access Control Policy and Procedures	LOW_MODERATE_HIGH	P1	The organization de	This control is intended to produce the policy and procedures that a		
Technical	Access Control	AC-2		Account Management	LOW_MODERATE_HIGH	P1	The organization m	The identification of authori	MODERATE_HIGH	The organ
Technical	Access Control	AC-3		Access Enforcement	LOW_MODERATE_HIGH	P1	The information sy	Access control policies (e.g.,	NONE	[Withdrav
Technical	Access Control	AC-4		Information Flow Enforcement	MODERATE_HIGH	P1	The information sy	Information flow control reg	NONE	The inforr
Technical	Access Control	AC-5		Separation of Duties	MODERATE_HIGH	P1	The organization: S	Examples of separation of duties include: (i) mission functions and		
Technical	Access Control	AC-6		Least Privilege	MODERATE_HIGH	P1	The organization er	The access authorizations de	MODERATE_HIGH	The organ
Technical	Access Control	AC-7		Unsuccessful Login Attempts	LOW_MODERATE_HIGH	P2	The information sy	Due to the potential for deni	NONE	The inforr
Technical	Access Control	AC-8		System Use Notification	LOW_MODERATE_HIGH	P1	The information sy	System use notification messages can be implemented in the form		
Technical	Access Control	AC-9		Previous Logon (Access) Notification	NONE	P0	The information sy	This control is intended to cc	NONE	The inforr
Technical	Access Control	AC-10		Concurrent Session Control	HIGH	P2	The information sy	The organization may define the maximum number of concurrent se		
Technical	Access Control	AC-11		Session Lock	MODERATE_HIGH	P3	The information sy	A session lock is a temporary	NONE	The inforr
Technical	Access Control	AC-12		Session Termination	NONE		[Withdrawn: Incorporated into SC-10].			
Technical	Access Control	AC-13		Supervision and Review Access Contr	NONE		[Withdrawn: Incorporated into AC-2 and AU-6].			
Technical	Access Control	AC-14		Permitted Actions Without Identifica	LOW_MODERATE_HIGH	P1	The organization: I	This control is intended for t	MODERATE_HIGH	The organ
Technical	Access Control	AC-15		Automated Marking	NONE		[Withdrawn: Incorporated into MP-3].			
Technical	Access Control	AC-16		Security Attributes	NONE	P0	The information sy	Security attributes are abstra	NONE	The inforr
Technical	Access Control	AC-17		Remote Access	LOW_MODERATE_HIGH	P1	The organization: D	This control requires explicit	MODERATE_HIGH	The organ
Technical	Access Control	AC-18		Wireless Access	LOW_MODERATE_HIGH	P1	The organization: E	Wireless technologies includ	MODERATE_HIGH	The inforr
Technical	Access Control	AC-19		Access Control for Mobile Devices	LOW_MODERATE_HIGH	P1	The organization: E	Mobile devices include porta	MODERATE_HIGH	The organ
Technical	Access Control	AC-20		Use of External Information Systems	LOW_MODERATE_HIGH	P1	The organization es	External information system	MODERATE_HIGH	The organ
Technical	Access Control	AC-21		User-based Collaboration and Inform	NONE	P0	The organization: F	The control applies to inform	NONE	The inforr
Technical	Access Control	AC-22		Publicly Accessible Content	LOW_MODERATE_HIGH	P2	The organization: D	Nonpublic information is any information for which the general pub		
Operational	Awareness and Tr	AT-1		Security Awareness and Training Poli	LOW_MODERATE_HIGH	P1	The organization de	This control is intended to produce the policy and procedures that a		
Operational	Awareness and Tr	AT-2		Security Awareness	LOW_MODERATE_HIGH	P1	The organization pr	The organization determines	NONE	The organ

Option #2

DHS CSET

With Spreadsheet, Word & file-sharing



IMPRIMIS INC

CTAM

iVACT 800 PRO

Option #3

i2ACT-800

MD MEP
MANUFACTURING EXTENSION PARTNERSHIP

MICHIGAN MANUFACTURING TECHNOLOGY CENTER

DIB
DEFENSE INDUSTRIAL BASE
CRITICAL INFRASTRUCTURE PROTECTION
INFORMATION SHARING AND ANALYSIS CENTER

CYBERVERIFY
DFAR COMPLIANT

IMPRIMIS ACT-

Assessment & Compliance Tool

DMDII
a UI LABS Collaboration

NATIONAL CYBERSECURITY CENTER
Response · Education
Training · Research

NATIONAL CYBER EXCHANGE

i2ACT Architecture & Configuration

BACK END DATABASE

- User Data

FRONT END DATABASE

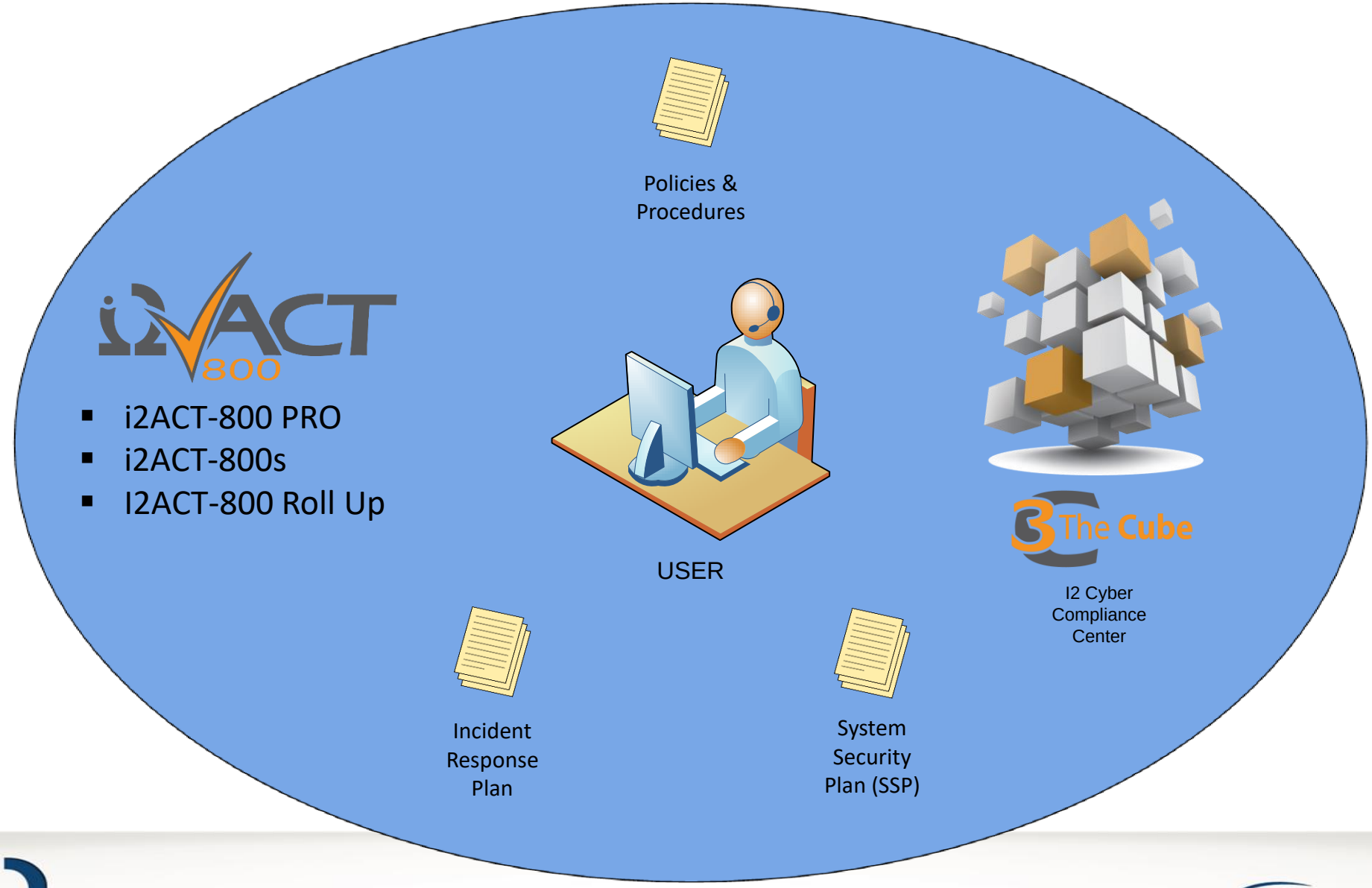
- User Interface
- Standards Database
- Queries
- Reports
- Baselines

COLLABORATION

Up to 20 people may work simultaneously

- TAB: Supplemental Guidance (NIST)
- TAB: Questionnaires
- TAB: Intent & Evidence
- TAB: How to Assess & Comply
- TAB: Remediation Plan & POA&M

The i2ACT Support Suite



SUMMARY

(Cyber) Dogs That Won't Hunt

- I'm a small company, no one is interested in what we do …
- I've got plenty of time – I'll do it next year …
- No one is going to check so I'll just fake it …
- I'm a small business, I don't need to be smart on cybersecurity …
- I went to the cloud so they do my cybersecurity …
- If the government get's hacked, they should not hold me to a standard …
- I am a small business, I can't afford cybersecurity …

NEW TERM:
CYBER ANTIBODIES – They kill or push the bad cells (systems) out …

Summary & Key Take-Aways

- The threat from the cyber domain is very, very real and it is ***our responsibility*** to deal with combatting this threat and managing the risk
- The need for cyber compliance is here ***now – today*** – and the Government Requirements are only going to grow, e.g. DFARS, FAR, CUI, etc.
- Baseline standards are required for classified and unclassified systems
- The DSS AAPM is the new standard for system accreditation or authorization
- NIST (SP) 800-171 is the minimum baseline standard for unclassified systems in contractor facilities
- The lack of provable cyber security compliance, represents a ***real and present danger to small businesses***
- Resources and tools exist to support the compliance process, and these tools will get better with time and with use

… This is Doable, You Can Make This Happen!!!!

IMPRIMIS, INC.

FOR ADDITIONAL INFORMATION

http://www.i2ComplianceTools.com

Michael G. Semmens

(719) 785-0333

Michael.Semmens@Imprimis-Inc.com

Turning Technology into Capability