January 28, 2016
ABA Public Contracts Law Section | State and Local Division

Federal Cyber Security Initiatives: Implications for State & Local Governments (and Contractors)

Robert S. Metzger
Rogers Joseph O'Donnell, P.C.
875 15th Street, N.W., Ste 725
Washington, D.C. 20005
(202) 777-8951
rmetzger@rjo.com www.rjo.com

Subjects

- Introduction & Overview
- What is to be protected: The CUI Rule
- What safeguards to employ: NIST SP 800-171
- Application to State and Local Governments
- Implications for SLED Contractors
- Parallel Measures of Sensitive State Information
- Getting a “Head Start”

Introduction & Overview

Protection of Information & Information Systems

"Many federal contractors, for example, routinely process, store, and transmit sensitive federal information in their information systems to support the delivery of essential products and services to federal agencies (e.g., providing credit card and other financial services; providing Web and electronic mail services; conducting background investigations for security clearances; processing healthcare data; providing cloud services; and developing communications, satellite, and weapons systems). **Additionally, federal information is frequently provided to or shared with entities such as State and local governments, colleges and universities, and independent research organizations."**

NIST SP 800-171 (Final), at 1-1.

The "Application Vector" to SLED

- The federal government is near a Final Rule on designation and safeguarding "Controlled Unclassified Information" (CUI).
- New cyber safeguards (NIST SP 800-171) were created to protect CUI in non-federal information systems.
- A "General FAR Rule" will require all federal agencies to require cyber protection of CUI, in accordance with SP 800-171, in contracts and agreements.
- As SLED entities execute agreements subject to these requirements, they (and their contractors) will be obligated to protect CUI per SP 800-171.
- Expect these obligations to initially arise in 2016.

Federal Information to Protect

E.O. 13556 makes the National Archives and Records Administration (**NARA**) responsible to determine what types of federal information require dissemination controls and protection. The focus is upon "Controlled Unclassified Information" or "**CUI**."

- **CUI** is federal information that requires protection pursuant to "laws, regulations, and Governmentwide policies."
- Many forms of CUI are provided to or used by state and local governments, and educational institutions ("SLED"). Areas =
  - Agriculture, Critical Infrastructure, Emergency Management, Financial, Geodetic, Immigration, Legal, Patent, Privacy, Proprietary Business, SAFETY Act, Statistical (Census), Tax, Transportation

Many forms of CUI are regularly provided to SLED recipients. The CUI security initiative is to safeguard that information when outside federal information systems.

Objective(s) of Protection

FISMA (P.L. 113-283) requires federal agencies to:

> "provide information security protections commensurate with the risk and the magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification or destruction of
>
> (A) information collected by or on behalf of an agency; or
>
> (B) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency"

- Federal agencies are obligated to assess impact of security breach on Confidentiality, Integrity & Availability (FIPS-199).
- As concern information and information systems of non-federal actors, the federal interest focuses on **confidentiality**.
- Threats to federal information include exfiltration, exploitation, unauthorized use; theft, improper access – e.g., **OPM breach.**

Safeguarding - I

- Policy:

> "Agencies must safeguard CUI in a manner that minimizes the risk of unauthorized disclosure while allowing for access by authorized holders."

- Includes both physical and cyber protection
  - Cyber includes both information and information systems
    - Federal agencies must protect IAW FIPS-199 and FIPS-200 (confidentiality, integrity & availability) … same applies to systems operated by or "on behalf of" the federal government.
    - FIPS-200 sets seventeen "families" of cyber safeguards.
    - NIST **SP 800-53** sets the mechanics to achieve.
  - Non-federal holders of CUI – e.g., contractors and SLED – will be subject to SP 800-171, which employs 14 of FIPS-200 "families."

CUI that non-federal actors use to produce a product, provide a service, or perform a function, will be subject to SP 800-171 – not SP 800-53.

Safeguarding - II

CYBER SAFEGUARD CONTROL "FAMILIES" (FIPS-200)				
Access Control **(AC)**	Awareness & Training **(AT)**	Audit & Accountability **(AU)**	Certification, Accreditation & Security Assmts **(CA)**	Configuration Management **(CM)**
Contingency Planning **(CP)**	Identification & Authentication **(IA)**	Incident Response **(IR)**	Maintenance **(MA)**	Media Protection **(MP)**
Physical & Environmental Protection **(PE)**	Planning **(PA)**	Personnel Security **(PS)**	Risk Assessment **(RA)**	System and Services Acquisition **(SA)**
System and Communications Protection **(SC)**	System and Information Integrity **(SI)**			

EXAMPLE:
Access Control (AC): Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

Shaded blocks not in SP 800-171

The 3-Part Federal Initiative to Safeguard CUI

Federal acts to protect sensitive but unclassified information have 3 elements:

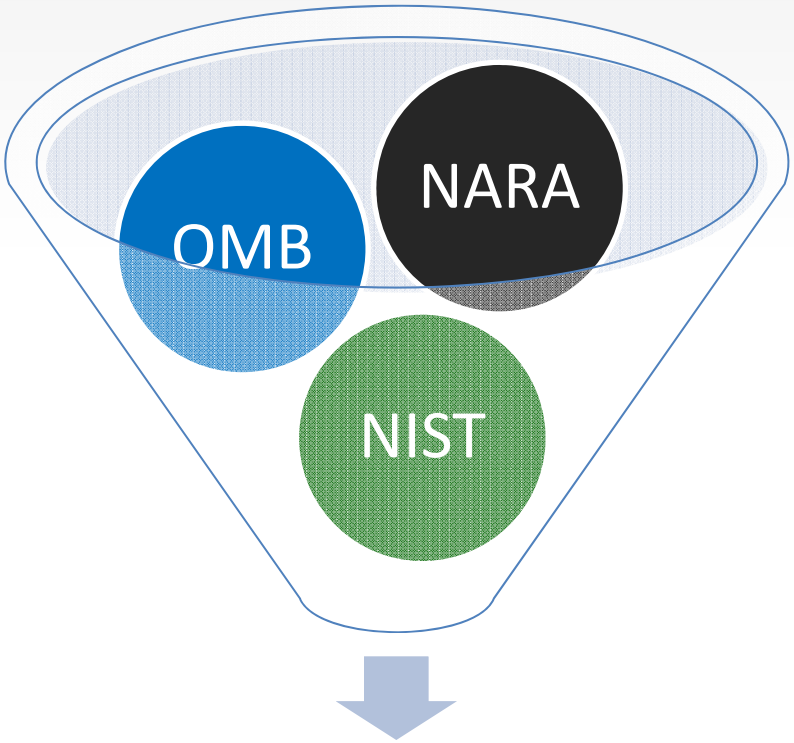
① NARA's proposed CUI Rule, establishing categories of CUI, responsibilities for designation, dissemination controls and required cyber security measures (which, when final, will point to NIST SP 800-171 for contractors and others who use CUI on non-federal information systems);

② NIST's SP 800-171, establishing cyber safeguards expected of commercial companies and other non-federal actors who host, use or transmit CUI; and

③ Acquisition Measures, effected by regulation, implemented through solicitation requirements and contract clauses, to obligate CUI recipients to protect CUI, e.g.,

- *DoD's "Unclassified Controlled Technical Information" DFARS (Nov. 2013), superseded by*
- *DoD's Interim Rule, "Network Penetration Reporting and Contracting for Cloud Services" (Aug. 2015, revised Dec. 2015)* – protects "Covered Defense Information" (CDI)
- *NARA's in-development "General FAR Rule" being developed by NARA for promulgation in 2016*

Federal Initiatives: Roles & Missions



ACQUISITION METHODS & CONTRACT CONTROLS - TOOLKIT

Responsibilities:

NARA: to define and categorize the varieties of "CUI" and establish workable guidelines & mechanisms

OMB ("8(e)" JWG): to decide on the mix of acquisition methods and contract tools

NIST: to identify required security controls and practices for adoption

Agencies: to evaluate cost/benefit, tailor, specify reporting, require monitoring, administer and oversee

SLED recipients of CUI will become subject to federal cyber obligations as these are imposed by contract or agreement term.

Applicability to SLEDs (how, when, why)

Today:
State and Local governments are not now subject to CUI safeguard requirements *unless* they receive DoD "Covered Defense Information" under a contract or other agreement subject to the new 'Network Penetration' DFARS.

Why?
FISMA imposes on the federal government a legal duty to protect information and provide information security regardless of whether that information is employed on a federal information system or by non-federal actors such as state and local governments, their contractors, educational institutions or otherwise.

So?
SLEDs should identify present receipt and use of CUI, assess their information systems for conformance with SP 800-171, and plan parallel measures for contracts to assure necessary protection. SLEDs can expect a transition period to allow for implementation.

Now?
All DoD contracts and subcontracts now require the DFARS 'Network Penetration' clause that obligates holders of "Covered Defense Information" to provide cyber protection per NIST SP 800-171 and to report to DoD cyber incidents. Some educational institutions (and perhaps states) will receive contracts from DoD (or DoD primes) subject to these obligations.

Soon:
When NARA completes the CUI Rule and the "General FAR Rule is promulgated, State and Local governments will enter into agreements with the federal government that include minimum cyber safeguard requirements applicable to *all* categories of CUI they receive pursuant to such agreements.

Categories of Controlled Unclassified Information

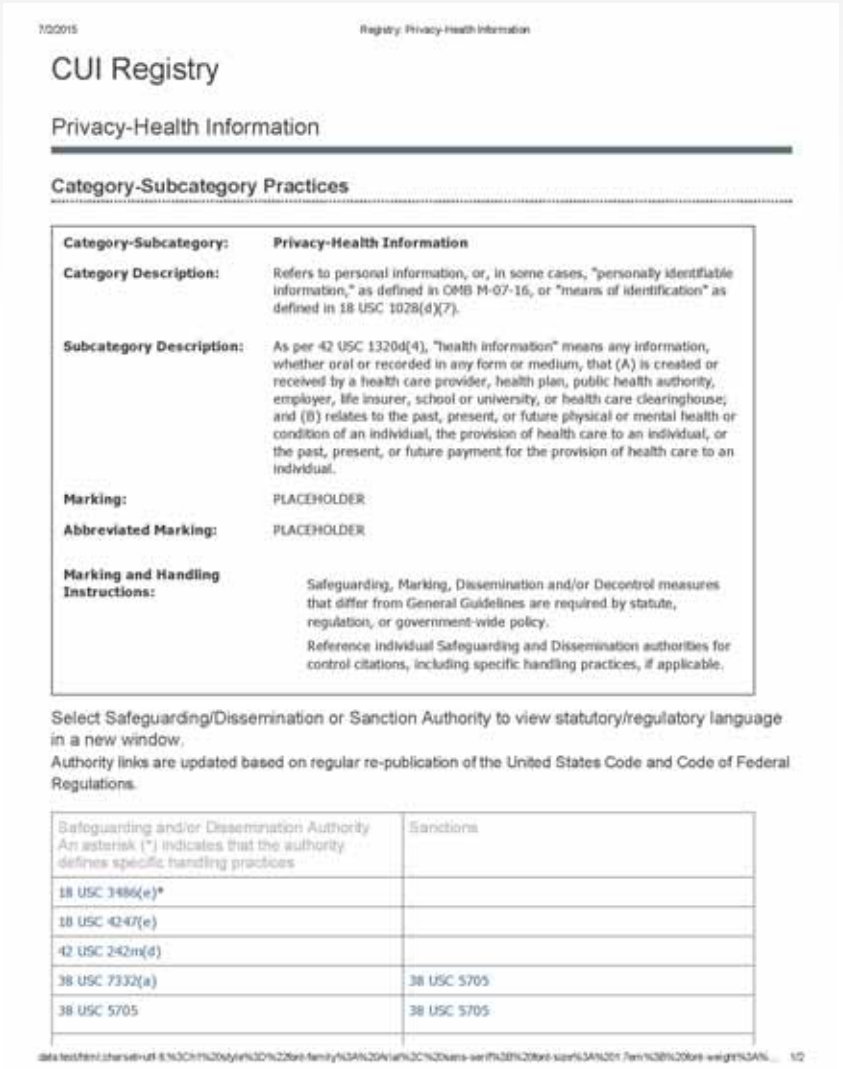
- Proposed rule ("Controlled Unclassified Information"), 32 CFR Part 2002 (May 8, 2015)
- The CUI Registry identifies 23 categories and 82 subcategories of CUI
- Who has access to CUI?
  - Federal Contractors
  - State and local governments
  - State and local contractors
  - Tribal governments
  - Colleges & Universities
  - Interstate Organizations
  - NGOs
  - Foreign governments

Agriculture	Controlled Technical Information	Critical Infrastructure (7 sub)	Emergency Management	Export Control (1 sub)
Financial (9 sub)	Foreign Government Information	Geodetic Product Information	Immigration (7 sub)	Information Systems Vulnerability
Intelligence (5 sub)	Law Enforcement (14 sub)	Legal (11 sub)	NATO (2 sub)	Nuclear (5 sub)
Patent (3 sub)	Privacy (8 sub)	Proprietary Business (5 sub)	SAFETY Act Information	Statistical (3 sub)
Tax (1 sub)	Transportation (1 sub)			

"CUI categories and subcategories are those types of information for which ***laws, regulations, or Government-wide policies*** requires safeguarding or dissemination controls". Proposed 32 C.F.R. § 2002.2 (Definitions)

NARA estimates that 300,000 contractors & grantees hold Controlled Unclassified Information

Health Information in the CUI Registry



7/2/2015 Registry: Privacy-Health Information

CUI Registry

Privacy-Health Information

Category-Subcategory Practices

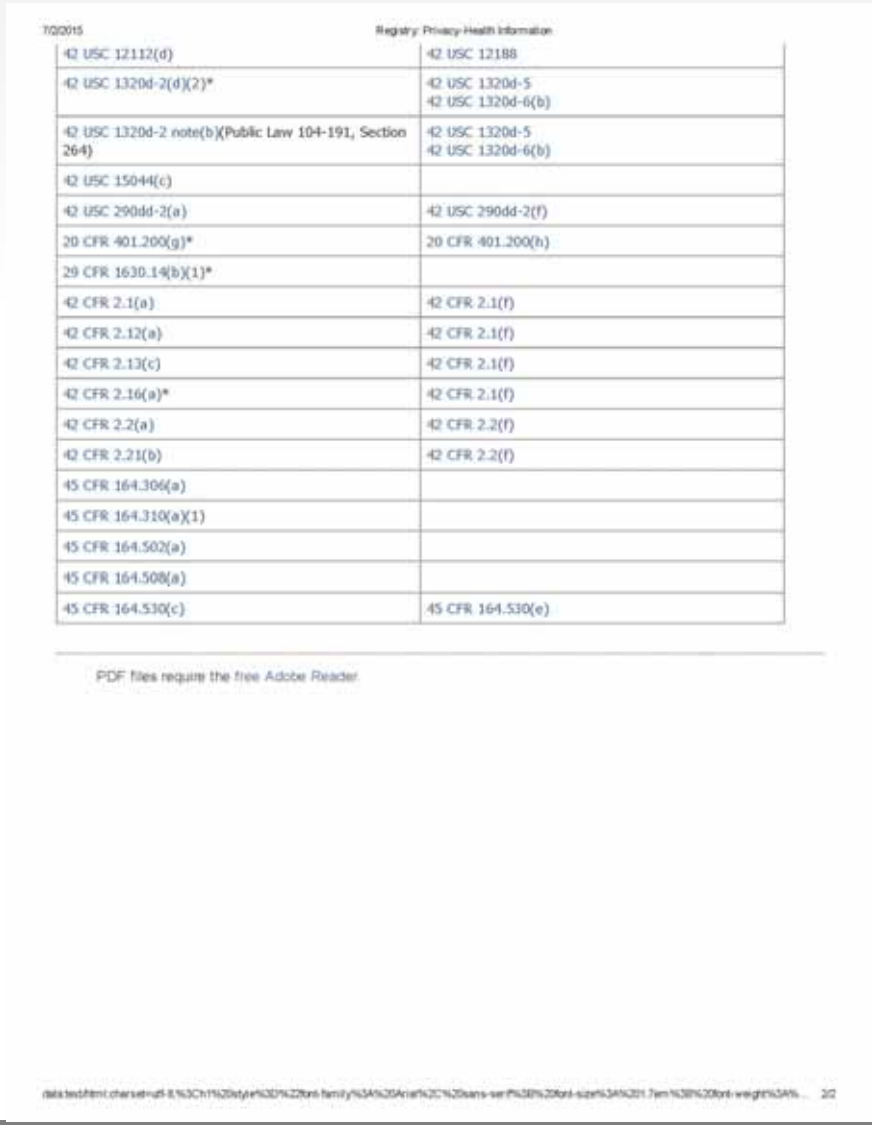
Category-Subcategory:	**Privacy-Health Information**
Category Description:	Refers to personal information, or, in some cases, "personally identifiable information," as defined in OMB M-07-16, or "means of identification" as defined in 18 USC 1028(d)(7).
Subcategory Description:	As per 42 USC 1320d(4), "health information" means any information, whether oral or recorded in any form or medium, that (A) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.
Marking:	PLACEHOLDER
Abbreviated Marking:	PLACEHOLDER
Marking and Handling Instructions:	Safeguarding, Marking, Dissemination and/or Decontrol measures that differ from General Guidelines are required by statute, regulation, or government-wide policy. Reference individual Safeguarding and Dissemination authorities for control citations, including specific handling practices, if applicable.

Select Safeguarding/Dissemination or Sanction Authority to view statutory/regulatory language in a new window.

Authority links are updated based on regular re-publication of the United States Code and Code of Federal Regulations.

Safeguarding and/or Dissemination Authority An asterisk (*) indicates that the authority defines specific handling practices	Sanctions
18 USC 3486(e)*	
18 USC 4247(e)	
42 USC 242m(d)	
38 USC 7332(a)	38 USC 5705
38 USC 5705	38 USC 5705

data:text/html;charset=utf-8,%3Ch1%20style%3D%22font-family%3A%20Arial%2C%20sans-serif%3B%20font-size%3A%201.7em%3B%20font-weight%3A%... 1/2



7/2/2015 Registry: Privacy-Health Information

42 USC 12112(d)	42 USC 12188
42 USC 1320d-2(d)(2)*	42 USC 1320d-5 42 USC 1320d-6(b)
42 USC 1320d-2 note(b)(Public Law 104-191, Section 264)	42 USC 1320d-5 42 USC 1320d-6(b)
42 USC 15044(c)	
42 USC 290dd-2(a)	42 USC 290dd-2(f)
20 CFR 401.200(g)*	20 CFR 401.200(h)
29 CFR 1630.14(b)(1)*	
42 CFR 2.1(a)	42 CFR 2.1(f)
42 CFR 2.12(a)	42 CFR 2.1(f)
42 CFR 2.13(c)	42 CFR 2.1(f)
42 CFR 2.16(a)*	42 CFR 2.1(f)
42 CFR 2.2(a)	42 CFR 2.2(f)
42 CFR 2.21(b)	42 CFR 2.2(f)
45 CFR 164.306(a)	
45 CFR 164.310(a)(1)	
45 CFR 164.502(a)	
45 CFR 164.508(a)	
45 CFR 164.530(c)	45 CFR 164.530(e)

PDF files require the free Adobe Reader

data:text/html;charset=utf-8,%3Ch1%20style%3D%22font-family%3A%20Arial%2C%20sans-serif%3B%20font-size%3A%201.7em%3B%20font-weight%3A%... 2/2

NIST SP 800-171: Control "Families"

SP 800-171 describes 30 "basic" and 79 "derived" security requirements. The "basic" requirements track to FIPS 200. The "derived" requirements reflect principles present in NIST 800-53 rev4.

Access Control (2/20)	Awareness & Training (2/1)	Audit & Accountability (2/7)	Configuration Management (2/7)	Identification & Authentication (2/9)
Incident Response (2/1)	Maintenance (2/4)	Media Protection (3/6)	Personnel Security (2/0)	Physical Protection (2/4)
Risk Assessment (1/2)	Security Assessment (3/0)	Systems & Comm Protection (2/14)	System & Information Integrity (3/4)	

SP 800-171 does not require submission of a Security Plan, for authorization or accreditation, or for review or approval.

Primary security objective: confidentiality

NIST SP 800-171 – and SLEDs

- SP 800-171 (Final) takes 14 of the 17 security "families" of FIPS 200 and extends these principles to contractors and others who host, use or transmit CUI.
- The security "requirements" of SP 800-171 are in the nature of "performance objectives" – not instructions, and not "prescriptive."
- Guidance is provided on "mapping" from other regimes to -171.
- SLED units and contractors with robust information security measures should have little trouble satisfying SP 800-171. Systems that already satisfy SP 800-53 will exceed SP 800-171 requirements.
- NIST (and NARA) specifically recognize that there are multiple sources and standards other than "federal."
- Protection of CUI by use of third party cloud providers is expected but the applicable (fed) safeguards are a "work in progress."

A Comparative Example

NIST SP 800-171
3.6 Incident Response

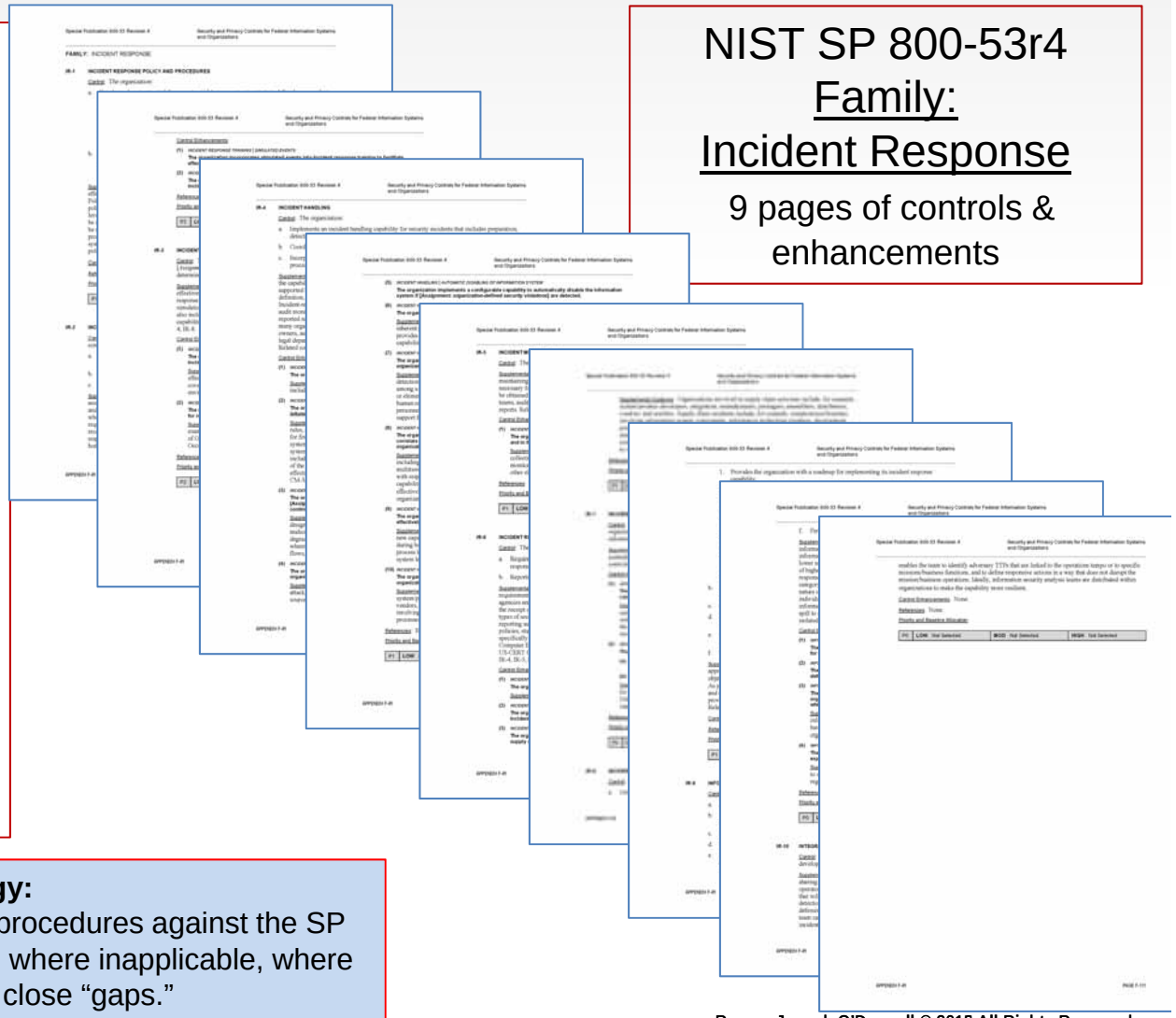
Basic Security Requirement

3.6.1 Establish an operational incident-handling capability for organizational information 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.

Derived Security Requirements

3.6.3 Test the organizational incident response capability.



NIST SP 800-53r4
Family:
Incident Response

9 pages of controls & enhancements

Response Strategy:
Assess existing systems, safeguards and procedures against the SP 800-171 "families" to determine where met, where inapplicable, where not – and to develop plans to close "gaps."

Potential Parallel Measures of State and Local Governments

Protection of "State Sensitive Information"?

- Premise:
  - Sensitive State (or Local) information ("SSI") merits protection for the same reasons as CUI.
  - State and Local Governments (SLGs) already seek assurance for information systems they operate or are operated by contractors on their behalf.
  - SLGs may seek to improve confidence that contractors or other recipients of "SSI," who use SSI to provide a service or perform a function, take measures to protect SSI confidentiality.
- Assumptions:
  - Public and private sector stakeholders have an interest in consistency and coherence in *what* is controlled and the *safeguards* employed.
  - Proliferation of safeguard "regimes" and conflicting obligations (even if similarly intended) would be costly, frustrating and potentially chaotic.
  - Most SSI users and recipients already have information systems security measures in place.
- Recommendations:
  - SLGs should follow the lead and learn from the federal government as it executes its CUI plan.
  - Cyber safeguards should converge on SP 800-171 as the "norm" for third party access to SSI (and CUI when received from SLGs), but allow for variations.
  - SLGs should avoid disproportionate or unrealistic obligation and risk-shifting.
  - Time will be needed for private sector participants to conform.

About the Presenter

This presentation reflects Mr. Metzger's personal views and should not be attributed to any client of his firm or organization with which he is involved or affiliated.

Robert S. Metzger
Rogers Joseph O'Donnell PC
202-777-8951
Rmetzger@rjo.com

Robert S. Metzger heads the Washington, D.C. office of Rogers Joseph O'Donnell, P.C., a boutique law firm that specializes in public procurement matters. He advises leading U.S. and international companies on key public contract compliance challenges and in strategic business pursuits. Bob is recognized for thought leadership in issues related to supply chain and cyber security. On these subjects, he has published extensively and has made presentations to many government, industry, legal and technical groups, among them ABA, AIA, ASIS, CALCE, DoD, DIB SCC, DoJ, DSB, ERAI, IPC, National IPR Center, NCMA, NDIA, SAE, SMTA and SSWG.

Bob is a Vice-Chair of the Cyber/Supply Chain Assurance Committee of the IT Alliance for Sector (ITAPs) (a unit of the Information Technology Industry Council).

Bob received his B.A. from Middlebury College and his J.D. from Georgetown University Law Center, where he was an Editor of the Georgetown Law Journal. He was a Research Fellow, Center for Science & International Affairs (now "Belfer Center"), Harvard Kennedy School of Government. Bob is a member of the International Institute for Strategic Studies (IISS), London. Academic publications on national security topics include articles in *International Security* and the *Journal of Strategic Studies*.

Taxonomy

- **CUI**: Controlled Unclassified Information
- **DFARS**: Defense Federal Acquisition Regulation Supplement
- **FAR**: Federal Acquisition Regulation
- **FIPS**: Federal Information Processing Standards
- **FISMA**: Federal Information Systems Modernization Act
- **GSA**: General Services Administration
- **NARA**: National Archives & Records Administration
- **NIST**: National Institute of Standards & Technology
- **OMB**: Office of Management and Budget
- **OPM**: Office of Personnel Management