Winvale

ROGERS JOSEPH O'DONNELL rjo

Cyber Threats & Privacy Concerns in the Public Sector

June 23, 2015

ROGERS JOSEPH O'DONNELL rjo

Meet the Presenters

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. He advises leading U.S. and international companies on key public contract compliance challenges and in strategic business pursuits. Bob is recognized as among the nation's leading experts in issues related to supply chain and cyber security. He is the Vice-Chair of the Software and Supply Chain Assurance Working Group of the IT Alliance for Sector (ITAPs), a unit of the Information Technology Industry Council.

Kevin Lancaster
CEO, Winvale
202-296-5505
Klancaster@winvale.com

Kevin Lancaster leads Winvale's corporate growth strategies in both the commercial and government markets. He develops and drives solutions to meet Winvale's business goals while enabling an operating model to help staff identify and respond to emerging trends that affect both Winvale and the clients it serves. He is integrally involved in all aspects of managing the firm's operations and workforce, leading efforts to improve productivity, profitability, and customer satisfaction.

Winvale

Agenda

- **The Cyber Threat to Federal Information**
- **What's At Stake for Commercial Companies**
- **Prudent Self-Assessment**
- **Incident Identification & Event Management**
- **Reporting: When To Share, What to Share**
- **Restoration: Getting Back to Work**
- **Remediation: Addressing Privacy Concerns**
- **What Not to Do Following a Cyber Attack**

The Cyber Threat to Federal Information

Information at Risk

- Classified Information
- **Controlled Unclassified information (23 categories, 82 subcategories)**
- Enterprise IP and proprietary information (e.g., PII, PCI)
- Personal privacy information (e.g., HIPAA)

Systems at Risk

- "Federal Information Systems"
- **"Non-federal Information Systems" (contractor systems)**
- "External Systems" (cloud)

Nature of the Threat

- Actors - range from hacker to state-sponsored actors or nation states
- Objectives – include annoyance, exfiltration, espionage, disruption/destruction
- Vectors – range from insider threats through external media to attrition

Consequences of Attack

- Data **Confidentiality**
- System Integrity
- Mission Availability

Categories of Controlled Unclassified Information

- NARA issued a proposed rule ("Controlled Unclassified Information"), 32 CFR Part 2002, on May 8, 2015 (80 Fed. Reg. 26501)

- The CUI Registry identifies 23 categories and 82 subcategories of CUI

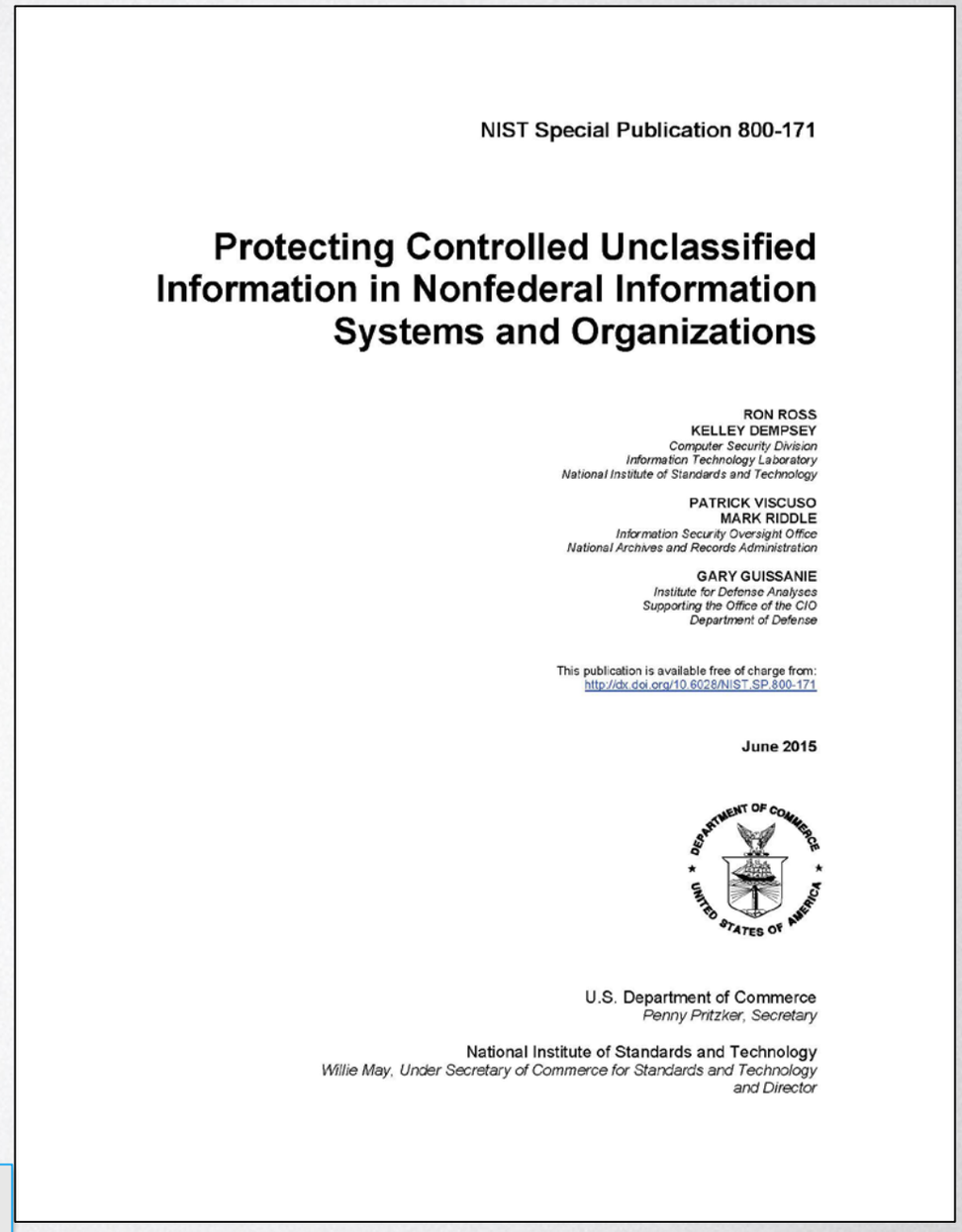
- Who has access to CUI?
  - Federal Contractors
  - State and local governments
  - State and local contractors
  - Tribal governments
  - Colleges & Universities
  - Interstate Organizations
  - NGOs
  - Foreign governments

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

The Federal Interest in CUI

"Today, more than at any time in history, the federal government is **relying on external service providers** to help carry out a wide range of federal missions and business functions using state-of-the-practice 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**. The **protection of sensitive federal information** while residing in *nonfederal information systems* and organizations is of **paramount importance** to federal agencies and can directly impact the ability of the federal government to successfully carry out its designated missions and business operations, including those missions and functions related to the critical infrastructure." NIST SP 800-171 (Final), at I-1.



NIST Special Publication 800-171

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

RON ROSS
KELLEY DEMPSEY
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

PATRICK VISCUSO
MARK RIDDLE
Information Security Oversight Office
National Archives and Records Administration

GARY GUISSANIE
Institute for Defense Analyses
Supporting the Office of the CIO
Department of Defense

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-171

June 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

NIST → NARA → JWG → FAR → **CONTRACTS**

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf

What's At Stake for Commercial Companies

The federal government will act to protect CUI that private companies host, use or transmit. Measures will affect:

- Companies who operate "federal information systems"
- Companies who use CUI on their own systems
- Companies who rely on "external" (cloud) providers

The OPM breach initially focuses scrutiny on the protection of federal information systems.

But information of the same or similar character and sensitivity is routinely held by commercial companies – and is at risk.

Expect cyber safeguards to become contract requirements. Contractors should prepare now for these obligations.

DoD and DHS already have CUI cyber measures in place.

Prudent Self-Assessment

Know types of information that are subject to federal law (e.g., Privacy Act, HIPAA), state law, other regulation or contract requirement.

Identify Categories of **CUI** in your system.

Consider and compare your safeguards against the 14 "families" of cyber "requirements" in NIST SP 800-171.

Develop and maintain a Cybersecurity Risk Management Plan (RMP).

Prepare an Incident Response Plan reflecting information at risk, applicable laws and regulations and specific contract requirements.

Secure Board-level or C-Suite approval. Monitor emerging federal requirements and execute Cyber RMP ahead of requirements.

Effective measures to protect CUI against cyber threats will be at least a positive competitive discriminator

Incident Identification & Event Management

Investigate use of continuous monitoring techniques.

Identify resources able to evaluate "incidents" and to determine whether an "event" is actionable.

Not always clear that an "incident" results in actionable privacy impact or contractual obligation.

- Involve technical and forensic specialists.
- Document investigation and to preserve records.
- Tension between state of knowledge and reporting obligations.

Procedures are needed to prioritize incident handing.

Identification should seek to determine event status, type, size, method, location, timing, data affected, impact, etc. Dimensions, vector, consequence, etc., may be very difficult to determine.

The Response Plan should involve senior management, assign responsibilities and include a detailed roadmap.

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.

Reporting: When To Share, What to Share

Know your reporting obligations – as a function of information type, contract obligation, federal and state law, impacted party.

Identify privacy risks present in potential disclosure; consider methods to "anonymize" disclosure of potentially sensitive data.

Evaluate obligations to report to federal sources such as US-CERT and to law enforcement. It may be prudent to involve counsel.

Have ready process to evaluate impact and make immediately necessary reports to all involved authorities.

Know in advance all potentially applicable reporting deadlines and the information content required for each.

Organizational responsibilities, decision making authority and reporting assignments should be established in advance.

*FISMA requires federal agencies to report within 1 hour of **confirmed** impact to confidentiality, integrity or availability.*

Specific reporting obligations may vary by contract and by agency requirement.
E.g., DoD UCTI: 72-hours; DHS (PCII, SSII or FOUO): 1-hour

Restoration: Getting Back to Work

A cyber event may be accompanied by system interruption or by question as to data integrity. This may expose a contractor to penalties, damages or even termination.

Federal contractors will be expected (or required) to restore functionality and validate data integrity. Companies should examine carefully specific "repair point objectives" and other contract requirements.

Consider NIST SP 800-171 or other methods to manage backup or other measures to reduce time to recover and return system to trustworthy operation.

Again expert 3d party resources should be identified.

US-CERT reports are to include impact to **recoverability** *and* **mitigation details**, *if any.*

Remediation: Addressing Privacy Concerns

Assess the information types at risk.

- Know the applicable privacy and disclosure obligations for each information type.
- Federal requirements include HIPAA, Privacy Act.
- At least 46 states have "breach" notice requirements.

Plan for attack scenarios. Have ready process for compliant notice and remediation for any affected individuals.

- Engage specialized 3d party resource skilled in leveraging experience to expedite and deliver necessary notification, identity protection and other remedial measures.
- Legal counsel is likely necessary to advise on reporting and compliance.

What Not to Do Following a Cyber Attack

- Do not start planning after the event has occurred.
- Do not wait for "perfect knowledge" before reporting.
- Do not debate before acting.
- Do not withhold key details from customers and cyber authorities.
- Do wait until after the event to inventory information types and the "domicile" of at-risk individuals.
- Do not destroy or compromise information potentially needed for diagnosis, forensics or investigation.
- Do not delay in getting notification to affected individuals and extending identity protection.
- Do not act without expert advice and support.

Questions?

Follow us on Twitter: @winvale
@robertmetzger2

ROGERS JOSEPH O'DONNELL rjo

About Winvale

For the past decade, Winvale has stood by its public and private sector customers providing cutting edge solutions from the world's leading technology vendors. Winvale provides Pre- Breach Intelligence (Dark Web Monitoring, Breach Response Planning) and Post- Breach Incident Response Management.

For more information, visit www.winvale.com or call (202) 296-5505.

Join Us for Our Next Webinar

Date: July 1, 2015 at 1:00 PM EST

Topic: *Selling to the Government - Session 2: Proposal & GovOpp Best Practices*

About RJO

RJO is a boutique government contracts firm with offices in San Francisco and D.C. We are the ranked in "Tier 2" by 2015 Chambers USA and "Band 2" by 2015 Legal 500 – the only boutique among the top U.S. firms. www.rjo.com