CRISIS MANAGEMENT AND FIRST AID: WHEN GOVERNMENT CONTRACTORS ARE THE HEADLINERS

WELCOME
CYBER CRISIS MANAGEMENT: ARE YOU PREPARED?

Evan Wolff
David Bodenheimer
Kelly Currie
Kate Growley
Overview

• Cybersecurity Framework and E.O. 13636 updates
• DoD’s NIST shift & DFARS requirements
• Cloud security, FedRAMP, & DoD’s special rules
• Unruly information security rules
• Responding to a data breach
• Managing legal, regulatory, business, and public relations implications after a data breach
Executive Order 13636

- § 7: Cyber standards for critical infrastructure
- § 8: Voluntary adoption program
- § 8(e): Explore possible FAR amendments
- § 10(a): Assess regulatory authorities
## The CSF Core

<table>
<thead>
<tr>
<th>Function Unique Identifier</th>
<th>Function</th>
<th>Category Unique Identifier</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Identify</td>
<td>ID.AM</td>
<td>Asset Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.BE</td>
<td>Business Environment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.GV</td>
<td>Governance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.RA</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.RM</td>
<td>Risk Management Strategy</td>
</tr>
<tr>
<td>PR</td>
<td>Protect</td>
<td>PR.AC</td>
<td>Access Control</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.AT</td>
<td>Awareness and Training</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.DS</td>
<td>Data Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.IP</td>
<td>Information Protection Processes and Procedures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.MA</td>
<td>Maintenance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.PT</td>
<td>Protective Technology</td>
</tr>
<tr>
<td>DE</td>
<td>Detect</td>
<td>DE.AE</td>
<td>Anomalies and Events</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE.CM</td>
<td>Security Continuous Monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE.DP</td>
<td>Detection Processes</td>
</tr>
<tr>
<td>RS</td>
<td>Respond</td>
<td>RS.RP</td>
<td>Response Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.CO</td>
<td>Communications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.AN</td>
<td>Analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.MI</td>
<td>Mitigation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.IM</td>
<td>Improvements</td>
</tr>
<tr>
<td>RC</td>
<td>Recover</td>
<td>RC.RP</td>
<td>Recovery Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.CO</td>
<td>Communications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.IM</td>
<td>Improvements</td>
</tr>
</tbody>
</table>
Defining “Adoption”

• DHS managing voluntary adoption program

“An organization adopts the CSF when it uses the concepts depicted by the CSF as a key part of its systematic process for identifying, assessing, prioritizing, and/or communicating:

– cybersecurity risks,
– current approaches and efforts to address those risks, and
– Steps needed to reduce cybersecurity risks as part of its management of the organization’s broader risks and priorities.”

• Sector-specific v. company-specific
• NIST & DHS public meetings
Government Contracting Impact

GSA/DOD Report

- Six major recommendations
  1. Baseline cybersecurity requirements
  2. Training
  3. Common definitions
  4. Devise risk management strategy → CSF
  5. Purchases from OEM, authorized reseller, trusted sources
  6. Increase government accountability → FISMA
- ABA Comments submitted
DoD’s Cyber Game-Changers

**DoD’s New Cyber Rules**

- DFARS Security Rule
- Death of DIACAP
- DoD’s Shift to NIST
- DoD’s Special Cloud
- DoD’s Patchwork Rules
Key Requirements

• Scope
  – “controlled technical information”
  – E.g., R&D data, specs, standards

• Minimum Security Controls
  – 51 mandatory controls (NIST 800-53)

• Incident Reporting
  – Within 72 hours of discovery
  – Damage assessments & data retention

• Subcontractor Flowdown
  – Commercial contractors also

DEPARTMENT OF DEFENSE
Defense Acquisition Regulations System
48 CFR Parts 204, 212, and 252
RIN 0750–AG47
Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified Controlled Technical Information (DFARS Case 2011–D039)
AGENCY: Defense Acquisition Regulations System, Department of Defense (DoD).
ACTION: Final rule.

78 Fed. Reg. 69273 (Nov. 18, 2013)
DFARS Rule on Safeguarding Data

Are You DFAR’ed?

• Broad Reach of DFARS Rule
  – All solicitations & contracts
  – Technical information everywhere
• Mandatory Controls
  – Comply – or else
  – PCO waiver: Can you get it?
• Incident Reporting
  – No safe harbor
  – Incident response team ready?
• Subcontractor Flowdown
  – Who reports what, where & to whom?

Noncompliance Risks?

Too Soon to Tell but . . . . .

• Default Termination
• Out of Competitive Range
• Lost Awards & Protests

What’s Next?

• Prime/Sub Disputes
• Debarment (e.g., L-3)
• FCA Claims (e.g., PlastiLam)
DoD’s Shift to NIST & FISMA

**Death of DIACAP**

- **Dying Slowly**
  - DoD participation in NIST process
  - DoD Instruction 8582.01 (June 2012)
  - DFARS Rule (Nov. 2013)
- **DoD Shifts to NIST/FISMA (Finally)**
  - “compulsory and binding” by statute (40 U.S.C. § 11331)
  - DoD Instruction 8510.01 (Mar. 2014)
  - DoD Instruction 8500.01 (Mar. 2014)
  - *But see* DFARS 239.7102-1 (Olden)

---

**DoD replaces DIACAP**

- FISMA & NIST recognized
- NIST Risk Management Framework adopted
- NIST security controls used
DoD Risk Framework

- **Step 1: CATEGORIZE System**
  - Categorize the system in accordance with the CNSSI 1253
  - Initiate the Security Plan
  - Register system with DoD Component Cybersecurity Program
  - Assign qualified personnel to RMF roles

- **Step 2: SELECT Security Controls**
  - Common control identification
  - Select security controls
  - Develop system-level continuous monitoring strategy
  - Review and approve the security plan and continuous monitoring strategy
  - Apply overlays and tailor

- **Step 3: IMPLEMENT Security Controls**
  - Implement control solutions consistent with DoD Component Cybersecurity architectures
  - Document security control implementation in the security plan

- **Step 4: ASSESS Security Controls**
  - Develop and approve Security Assessment Plan
  - Assess security controls
  - SCA prepares Security Assessment Report (SAR)
  - Conduct initial remediation actions

- **Step 5: AUTHORIZE System**
  - Prepare the POA&M
  - Submit Security Authorization Package (security plan, SAR and POA&M) to AO
  - AO conducts final risk determination
  - AO makes authorization decision

- **Step 6: MONITOR Security Controls**
  - Determine impact of changes to the system and environment
  - Assess selected controls annually
  - Conduct needed remediation
  - Update security plan, SAR and POA&M
  - Report security status to AO
  - AO reviews reported status
  - Implement system decommissioning strategy

NIST on Steroids?

**DoD Theory**
- Harmony with NIST
- Deductive DIACAP changes

**Implementation Reality**
- Same DoD security staff
- Decades of DIACAP history
- DoD Cloud vs. FedRAMP
- Watch Out!
DoD’s Special Cloud

DoD Cloud Controls

Table of Contents

Appendix H  Control Parameters Annex ......................................................... H-1
1  Access Controls ................................................................. H-1
2  Awareness and Training Controls ........................................... H-4
3  Audit and Accountability Controls .......................................... H-4
4  Security Assessment and Authorization Controls ..................... H-6
5  Configuration Management Controls ...................................... H-7
6  Contingency Planning Controls ............................................... H-10
7  Identification and Authentication Controls ............................. H-12
8  Incident Response Controls .................................................. H-13
9  Maintenance Controls ............................................................ H-13
10  Media Protection Controls ................................................... H-13
11  Physical and Environmental Protection Controls .................... H-15
12  Planning Controls ................................................................. H-16
13  Personnel Security Controls ................................................ H-16
14  Risk Assessment Controls .................................................... H-17
15  System and Services Acquisition Controls ............................ H-18
16  System and Communications Protection Controls .................. H-18
17  System and Information Integrity Controls ............................ H-22

115
DoD’s Special Cloud

DoD Cloud Controls

- Centralized Control
  - DISA as Cloud Service Broker

- Scope
  - Commercial Cloud Services
  - Low Impact only

- Security Controls
  - Over & above FedRAMP
  - Matrix of controls

DoD Policy Memo

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
COMMANDERS OF THE COMBATANT COMMANDS
DIRECTOR, COST ASSSESSMENT AND PROGRAM EVALUATION
DIRECTOR, OPERATIONAL TEST AND EVALUATION
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Supplemental Guidance for the Department of Defense’s Acquisition and Secure Use of Commercial Cloud Services

References:
(b) Defense Information Systems Network Global Information Grid Flag Panel Charter, April 2012

This memorandum provides supplemental guidance for the acquisition and secure use of commercial cloud services in the DoD. The DoD Chief Information Officer (CIO) established Defense Information Systems Agency (DISA) as the Enterprise Cloud Service Broker to consolidate enterprise demand to manage the acquisition and delivery of the Department’s commercial cloud services, and to ensure a secure and efficient DoD cloud environment, reference 63. The broker will facilitate and optimize DoD’s access and use of commercial cloud services that can meet our security and interoperability requirements.

On June 25, 2013, the Defense Information Systems Network (DISN) Global Information Grid (GIG) Flag Panel authorized DISA as the Enterprise Cloud Service Broker with the responsibility of issuing DoD provisional authorizations for Department-wide use of commercial cloud services for low-impact data and missions, in accordance with reference (b). The DISN GIG Flag Panel decided that use of commercial cloud services for moderate-risk data or missions, which include Controlled Unclassified Information, require DISN GIG Flag Panel approval, coordinated via the Broker. As such, the Broker developed a DISN GIG Flag Panel approval process for issuing DoD provisional authorizations for commercial cloud services, based on input and review of DISA’s cyber security assessment by the Defense Information Assurance Security Accreditation Working Group.
DoD’s Special Cloud

DoD Cloud Matrix

- **Physical Access**
  - DoD access to CSP data center

- **Personnel Access**
  - U.S. citizens only

- **Nondisclosure Agreements**
  - NDAs for all CSP personnel

- **Indemnification**
  - CSPs indemnify DoD

- **Insurance**
  - CSPs must have cyber insurance

Acquisition Issues

- **Commercial Items**
  - Standard commercial practices

- **Competition**
  - Unduly restrictive specifications

- **FedRAMP**
  - Government-wide program

- **Executive Order**
  - Harmonization of standards

- **Public Notice & Comment**
  - APA standards
DoD’s Cyber Crazy Quilt

- **NDAA § 941**
  - “Rapid reporting” requirement
  - “successful penetration”

- **DFARS Safeguarding Rule**
  - Reporting within 72 hours of discovery
  - “possible exfiltration, manipulation”

- **DoD Cloud Policy**
  - Notify DoD within 60 minutes
  - Reporting a “breach” of data

- **DoD Healthcare Data**
  - HIPAA reporting requirements

Harmonization = Good

- **Cyber Executive Order**
  - Objective for harmonization

- **DoD/GSA Report**
  - Better security with consistent security rules

- **FedRAMP**
  - Government-wide
  - Approve once, use often

- **ABA Comments**
  - Need for harmonization
FedRAMP Changes Coming

FedRAMP 2.0

• **Security Controls**
  – Low & Moderate impact only
  – Not High impact (only 20% = high)

• **Personnel Access**
  – Add additional security controls
  – Update to NIST 800-53, Rev. 4

• **Federal Agencies & FedRAMP**
  – Many agencies not adding controls

FedRAMP Changes

“The General Services Administration is updating government-wide standards for securing cloud solutions and expects to release those changes within the next three months. The 298 security controls under FedRAMP are based on National Institute of Standards and Technology guidelines, which govern how agencies should secure their information technology systems. NIST updated those guidelines last year. GSA will release plans in the coming weeks for cloud providers under FedRAMP to transition to the new standards, said Matt Goodrich, program manager for FedRAMP.”

## Anatomy of a Cyber Event

<table>
<thead>
<tr>
<th>Pre-Incident Programs</th>
<th>Incident Response</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop and implement compliance program</td>
<td>Establish investigation team</td>
<td>Defend against regulatory enforcement actions</td>
</tr>
<tr>
<td>Policies and procedures</td>
<td>Retain technical consultants (under privilege)</td>
<td>Defend against class action litigation</td>
</tr>
<tr>
<td>Organization, management and audit functions</td>
<td>Disseminate a legal hold</td>
<td>Manage disputes with third parties</td>
</tr>
<tr>
<td>Electronic discovery &amp; information management</td>
<td>Identify and analyze risks</td>
<td>Coordinate on criminal prosecution</td>
</tr>
<tr>
<td>Analyze and understand cyber risks</td>
<td>Litigation</td>
<td></td>
</tr>
<tr>
<td>Define regulatory requirements</td>
<td>Data loss</td>
<td></td>
</tr>
<tr>
<td>Identify baseline threats</td>
<td>Restoration activities</td>
<td></td>
</tr>
<tr>
<td>Evaluate vulnerabilities</td>
<td>Review and comply with current policies and procedures</td>
<td></td>
</tr>
<tr>
<td>Analyze consequences</td>
<td>Review and comply with third party requirements</td>
<td></td>
</tr>
<tr>
<td>Incident response and crisis management</td>
<td>Media and PR communications</td>
<td></td>
</tr>
<tr>
<td>Privacy and data security, including handling of specific information types</td>
<td>Government interface</td>
<td></td>
</tr>
<tr>
<td>Analyze cyber insurance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contractual obligations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Training</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information sharing programs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use of comprehensive response technologies and optimization of data</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Interested Agencies

• Law Enforcement: FBI, DHS/U.S. Secret Service
• SEC – Reporting and governance
• FTC – Recent ‘fairness’ cases
• DHS – Voluntary adoption programs
• Critical Sector Lead Agencies:
  – DOE/FERC
  – DOT
  – USCG
Law Enforcement Resources

“[I]n the future, resources devoted to cyber-based threats will equal or even eclipse the resources devoted to non-cyber based terrorist threats.”

-- FBI Director James B. Comey
November 14, 2013
Government Response: Coordination and Connecting the Dots

National Cyber Investigative Joint Task Force (NCIJTF)

- 19 Agencies, led by FBI
- Includes NSA, CIA, other Intelligence Agencies
- Includes DHS, U.S. Secret Service
- Includes military components
- Liaison with Foreign counterparts
Coordination and Connecting the Dots

National Cybersecurity & Communications Integration Center (NCCIC)

• DHS led
• Federal departments, agencies, state & locals
• Private Sector, International entities
• Information Sharing, Prevention; Not Investigations & Enforcement
Do You Know Your Local Cyber Task Force?

- Cyber Task Forces (56 Across the Country)
  - Investigations of Cyber Crimes
  - Active Outreach to Private Sector, Universities, etc.
  - Best Practices, Information Sharing
  - Classified Threat Briefings

- 24-Hour Command Center – CyWatch
  - Email: cywatch@ic.fbi.gov or
  - Voice: +1-855-292-3937
The Prosecutors

Department of Justice
Computer Crimes Intellectual Property Section (CCIPS)

U.S. Attorney’s Offices (e.g. EDVA, DC, MD)
Before Your (Next) Cybersecurity Incident

• Does your Information Security Officer Know Who to Contact?

• Does Your Inside or Outside Counsel Know the Prosecutors?
  – DOJ/CCIPS
  – US Attorney’s Offices
Questions?

David Bodenheimer  202-624-2713  
\texttt{dbodenheimer@crowell.com}

Kate Growley  202-624-2698  
\texttt{kgrowley@crowell.com}

Kelly Currie  212-895-4257  
\texttt{kcurrie@crowell.com}

Evan Wolff  202-624-2615  
\texttt{ewolff@crowell.com}