PROGRAM MATERIALS
Program #2978
May 21, 2019

Cybersecurity: What Government Contractors Need to Know

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969

SheppardMullin

Cybersecurity:
What Government Contractors Need to Know

JONATHAN MEYER TOWNSEND BOURNE

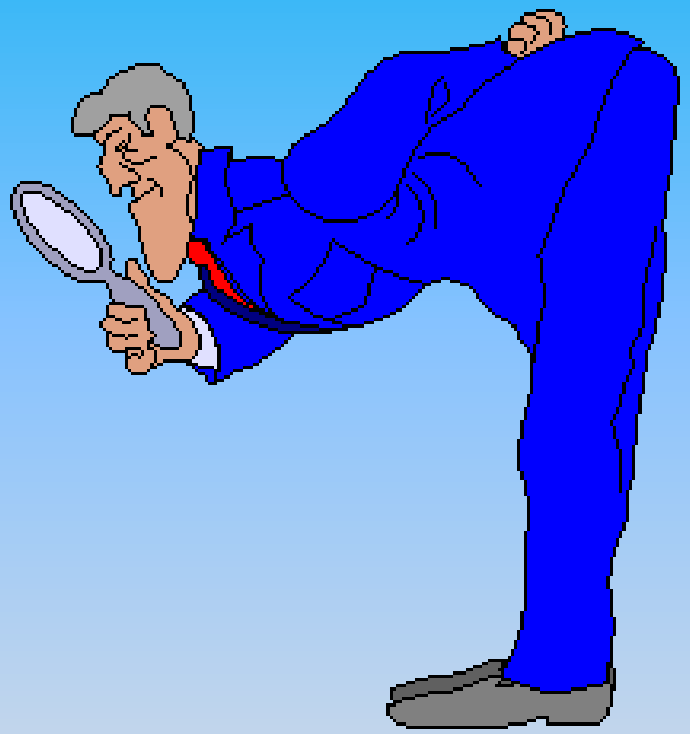
Nice to Meet You

Jonathan Meyer
T: 202.747.1920
jmeyer@sheppardmullin.com

Townsend Bourne
T: 202.747.2184
tbourne@sheppardmullin.com

Overview of Today

1. The Threat
2. The Data
3. The Laws
4. PII
5. The Privacy Act
6. Other Types of Information
7. FISMA
8. CUI
9. NIST
10. FAR and DFARS Clauses
11. The Cloud
12. Insider Threat



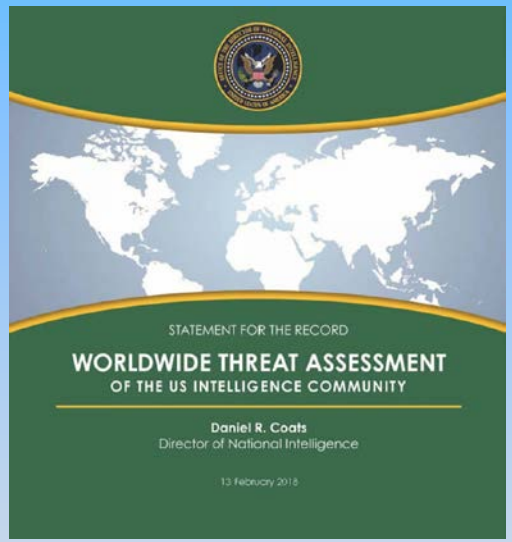
The Threat

The Changing Landscape…

Yearly "Worldwide Threat Assessment of the US Intelligence Community"

- 2007, no mention of cyber
- 2008, first mention ever of cyber as a threat
- 2016, first global threat discussed
  - even before terrorism
- 2018, continues to be first global threat

> *"The potential for surprise in the cyber realm will increase in the next year and beyond as billions more digital devices are connected…and both nation states and malign actors become more emboldened and better equipped in the use of increasingly widespread cyber toolkits."*



Developments in 2018 & 2019

- 2018 National Defense Authorization Act
  - Prohibition of Kaspersky software products and services
  - Now part of the FAR
- Cyber Digital Task Force Report (July 2018)
  - Focus on “malign foreign influence operations” and election interference
- 2019 National Defense Authorization Act
  - Includes restrictions on procurements based on ties to certain Chinese companies (*e.g.*, Huawei, ZTE Corporation)

By the Numbers

Data Records Are Lost Or Stolen At The Following Frequency:

Every Day

6,107,746

Records

Every Hour

254,489

Records

Every Minute

4,241

Records

Every Second

71

Records

Source: Breach Level Index (*last visited* January 11, 2019)

Motivations for Cyber Attacks

Financial Gain	Ideology/Terrorism
Espionage	Adventure/Thrill
Blackmail	Compulsive or Destructive Behavior
Negligence	Divided Loyalties
Revenge/Disgruntlement	Fame/Ego/Self-Image/Recognition

"The fact that people are full of greed, fear, or folly is predictable. The sequence is not predictable."
~Warren Buffett

There is no typical attack, but…

Compromise
- human error, ignorance or malice
- vendor systems

Escalation of Privileges

Internal Reconnaissance

Damage to Systems

Data Access

Data Acquisition

Potential Breach Impacts

- Financial loss
  - Direct
  - Indirect
- Reputational harm
- Loss of Intellectual Property (IP)
- Harm to national security and/or public safety
- Identity theft
- Legal Liability
- Suspension/Debarment

The Data

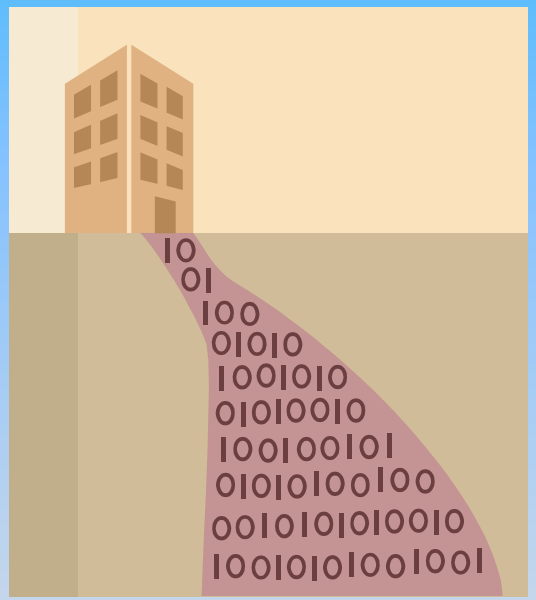
What Are “They” Seeking?

- Personally Identifiable Information (PII)
  - First name, last name, plus Social Security number
  - First name, last name, plus Driver’s License #
  - User name and email address (California only)

- Payment Card Information (PCI)
  - Credit Card Data
  - Bank account and PIN Information
  - Account user name and password

What Are “They” Seeking?

- Corporate Confidential Information
  - Trade Secrets
  - Customer Data / Contracts
  - Product Pricing / Share Pricing
  - “Secret Sauce”
  - Pending Mergers / Acquisitions / Targets
- Government Confidential Information
  - CUI
  - CDI
  - Etc.



The Laws

Cybersecurity Legal Framework

- **Overarching Federal Requirements:**
  - Computer Fraud and Abuse Act
  - Homeland Security Act of 2002
  - FTC Act
  - SEC Guidelines
  - Sarbanes-Oxley
  - Cybersecurity E.O. and BOD
  - Other Industry-Specific laws (FACTA, HIPAA, etc.)
  - Agency-specific regulations
  - National Defense Authorization Acts

Cybersecurity Legal Framework

- State Laws, *e.g.*:
  - New York – Department of Financial Services
  - South Carolina – breach notice requirements for insurance companies
  - California Consumer Protection Act – to take effect January 1, 2010
- International Regulations
  - General Data Protection Regulation (GDPR)

Determining Applicable Laws and Regulations

- Requirements applicable to you depend upon:
  - Data type and classification
  - Type of customer
  - Government funding
  - Contract scope of work

    - E.g., Contractors managing systems “on behalf of” the government v. non-federal systems
    - Cloud service providers

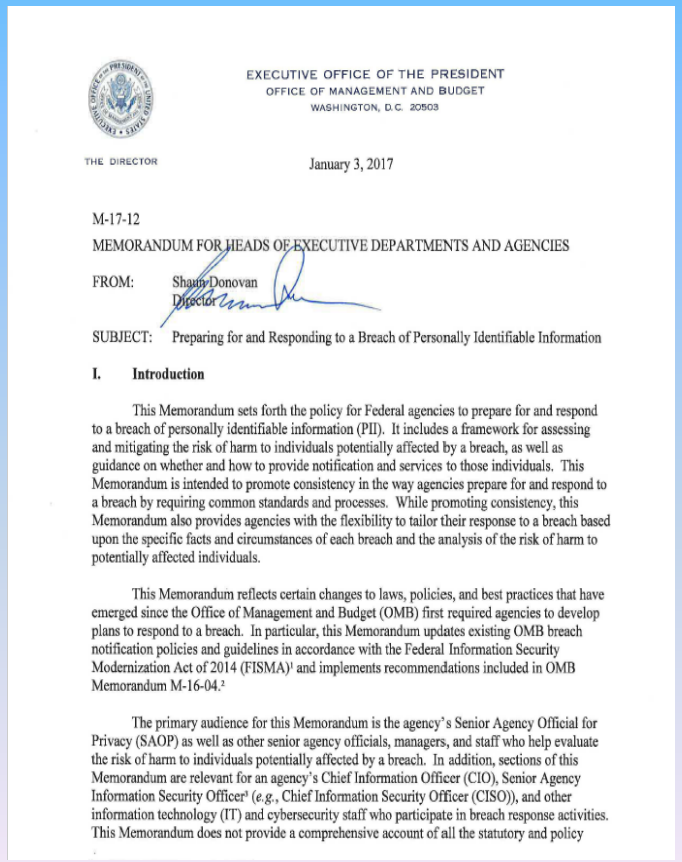
Potential Legal Consequences/Liability

- Federal lawsuit
- Bid protests
  - *E.g.*, alleged failure to comply with solicitation requirements for cybersecurity
- False Claims Act
  - *E.g.*, failure to disclose noncompliance or failure to report incident
- Suspension/Debarment
- Non-responsibility determination
- Negative CPAR ratings

Personally Identifiable Information (PII)

Personally Identifiable Information (PII)

- Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual."
  - OMB Memorandum M-17-12, Jan. 3, 2017
  - *E.g.*, name, social security number, biometrics data, date and place of birth, mother's maiden name, etc.
  - Change from 2007 definition – other information need not be personal or identifying, just linked or linkable
  - Recognizes agencies need to assess information over time; information that was once non-linkable may become so over time or from other sources



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

January 3, 2017

M-17-12

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shaun Donovan
Director

SUBJECT: Preparing for and Responding to a Breach of Personally Identifiable Information

I. Introduction

This Memorandum sets forth the policy for Federal agencies to prepare for and respond to a breach of personally identifiable information (PII). It includes a framework for assessing and mitigating the risk of harm to individuals potentially affected by a breach, as well as guidance on whether and how to provide notification and services to those individuals. This Memorandum is intended to promote consistency in the way agencies prepare for and respond to a breach by requiring common standards and processes. While promoting consistency, this Memorandum also provides agencies with the flexibility to tailor their response to a breach based upon the specific facts and circumstances of each breach and the analysis of the risk of harm to potentially affected individuals.

This Memorandum reflects certain changes to laws, policies, and best practices that have emerged since the Office of Management and Budget (OMB) first required agencies to develop plans to respond to a breach. In particular, this Memorandum updates existing OMB breach notification policies and guidelines in accordance with the Federal Information Security Modernization Act of 2014 (FISMA)[1] and implements recommendations included in OMB Memorandum M-16-04.[2]

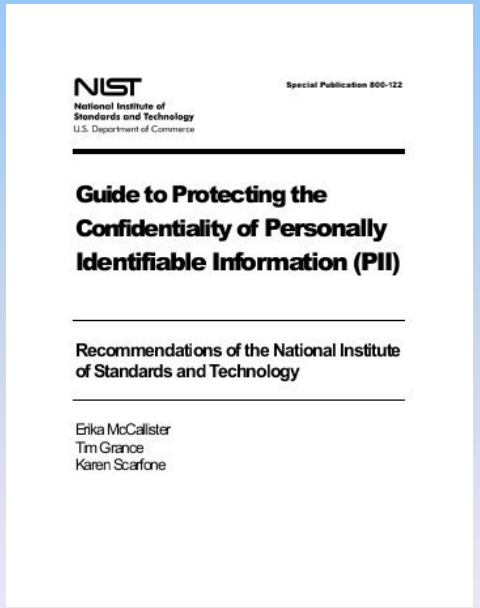
The primary audience for this Memorandum is the agency's Senior Agency Official for Privacy (SAOP) as well as other senior agency officials, managers, and staff who help evaluate the risk of harm to individuals potentially affected by a breach. In addition, sections of this Memorandum are relevant for an agency's Chief Information Officer (CIO), Senior Agency Information Security Officer[3] (*e.g.*, Chief Information Security Officer (CISO)), and other information technology (IT) and cybersecurity staff who participate in breach response activities. This Memorandum does not provide a comprehensive account of all the statutory and policy

Personally Identifiable Information (PII) (cont.)

- "[A]ny information about an individual…including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."

  - NIST SP 800-122, Guide to Protecting the Confidentiality of PII

  - "[A] list containing only credit scores without any additional information concerning the individuals to whom they relate does not provide sufficient information to distinguish a specific individual…. [I]f the list of credit scores were to be supplemented with information, such as age, address, and gender, it is probable that this additional information would render the individuals identifiable."


NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-122

Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

Recommendations of the National Institute of Standards and Technology

Erika McCallister
Tim Grance
Karen Scarfone

PII in the States

- Definitions of “personal information” differ among states
  - *E.g.*, login credentials such as usernames, email addresses, and passwords are considered personal information
    - CA, FL, IL, NE, NV, RI, WY
  - *E.g.*, biometric data (e.g., fingerprint, retina, or iris “measurements”)
    - IL, CA
  - *E.g.* data from an automated license plate recognition system
    - CA

- Note states also may have different reporting requirements

The Privacy Act

The Privacy Act of 1974, 5 U.S.C. § 552a

- Created in response to concerns about the impact of the use of computerized databases on individuals' privacy rights.
- Attempts to strike a balance between the Government's right to maintain information on individuals and the individual's right to have his or her privacy protected against unwarranted intrusions.
- Applies only to U.S. Persons.
- Limits an Agency's collection and sharing of personal data. Relates to when an Agency:
  - Collects personal information
  - Creates databases containing personal identifiers
  - Maintains databases containing personal identifiers
  - Disseminates information containing personal data

The Privacy Act Applied to Contractors

- Section (m) – applies Act to contractors that operate a system of records on behalf of an agency
- Privacy Act also will apply under contracts explicitly requiring compliance with the Privacy Act

> *The Contractor is bound by Section (m) of the Privacy Act, 5 U.S.C. Sec. 552a(m) and as such is considered under the act to be an employee of the agency. Accordingly, the Contractor and any of its employees are subject to the criminal penalties of the Privacy Act, 5 U.S.C. Sec.552a(i).*

- Violations of the Privacy Act may result in criminal penalties

The FAR

- FAR Part 24 – applies requirements of the Privacy Act and OMB Circular No. A-130 to government contracts
- The following clauses apply "[w]hen the design, development, or operation of a system of records on individuals is required to accomplish an agency function"
  - FAR 52.224-1, Privacy Act Notification – informs contractor it is subject to the Privacy Act and may be subject to criminal penalties for violations
  - FAR 52.224-2, Privacy Act – contractor agrees to comply with the Privacy Act and related regulations
    - Contractor considered an employee of the agency for purposes of civil or criminal actions
    - Flowdown to subcontractors that also design, develop, or operate system of records

The FAR Privacy Training Rule

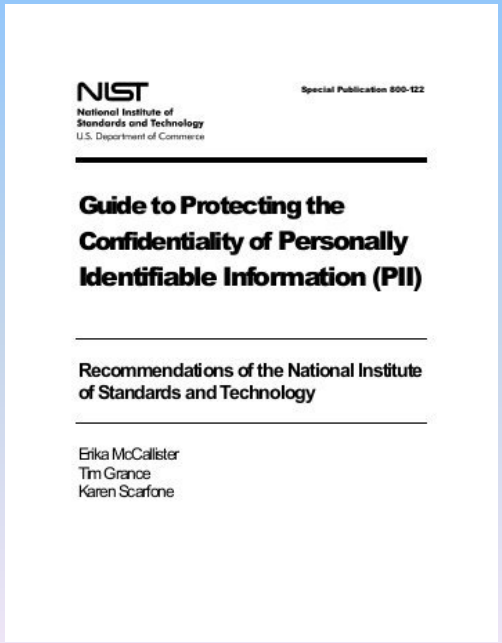
- FAR 52.224-3, Privacy Training – applies where employees will:
  - (1) Have access to system of records;
  - (2) Create, collect, use, etc. PII; or
  - (3) Design, develop, maintain, or operate a system of records
- Minimum training requirements:
  - Provisions of the Act including penalties for violations;
  - Appropriate handling and safeguarding of PII;
  - Authorized use of a system of records or PII;
  - Restrictions on use of unauthorized equipment to handle or access PII;
  - Prohibitions on unauthorized use of a system of records or unauthorized access or handling of PII; and
  - Incident response procedures for suspected or confirmed breaches of a system of records or unauthorized disclosure or access of PII.

FAR 52.239-1, Privacy or Security Safeguards

- Applies Privacy Act to certain IT contracts
  - Required in contracts for "security of information technology, and/or are for the design, development, or operation of a system of records using commercial information technology services or support services"
- Contractor is not to share details regarding safeguards relating to the contract
- Disclosure requirement: "If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party."
- No flow-down to subcontractors

NIST SP 800-122

- NIST SP 800-122, Guide to Protecting the Confidentiality of PII
  - Identify your PII
  - Minimize collection to only necessary PII
  - Categorize PII (low, moderate, high); *e.g.*, identifiability, quantity, access
  - Safeguard PII
  - Develop incident response plan


NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-122

Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

Recommendations of the National Institute of Standards and Technology

Erika McCallister
Tim Grance
Karen Scarfone

OMB Memorandum M-17-12

- "Preparing for and Responding to a Breach of Personally Identifiable Information" – 1/3/17
- Breach response and preparedness standards for contractors who are (1) collecting or maintaining PII, or (2) using or maintaining an information system on behalf of the Government.
  - **Encrypt PII**;
  - **Report breaches** (including *unconfirmed*) without unreasonable delay;
  - **Regular training** for contractor employees on how to identify and report a breach;
  - Maintain capabilities to **track the access to information** (including the time of access and the identity of the party accessing the information), construct a timeline of activity, and identify attack vectors;
  - **Cooperate with the agency**, including any necessary exchange of information, in order to effectively report and manage a suspected breach;
  - **Allow for inspection**, investigation, forensic analysis, etc.; and
  - **Identify roles and responsibilities** consistent with the policy and with the agency's breach response plan.
  - The contract must also state that a breach, by itself, shall not be interpreted as evidence of a failure to provide adequate safeguards for PII

Other Specific Types of Information (PHI, etc.)

Protected Health Information (PHI)

- **PHI**: Individually identifiable health information relating to (i) past, present, or future physical or mental health or condition; (ii) the provision of healthcare; or (iii) the past, present, or future payment for the provision of healthcare.

- **Health Insurance Portability and Accountability Act (HIPAA)** – Enforced by the Department of Health and Human Services (HHS), Office for Civil Rights (OCR); state attorneys general may bring suit in federal courts on behalf of their residents.

  - **HIPAA Security Rule:** Establishes minimum security requirements, but emphasizes that security measures must be "reasonable" based on an initial and ongoing risk assessment.

  - **Security Incident**

    - Only report a security incident if it is a breach

      - A breach of PHI is the acquisition, access, use, or disclosure of *unsecured* PHI, in a manner not permitted by HIPAA, *which* poses a significant risk of financial, reputational, or other harm to the affected individual.

      - A breach is presumed unless there is a minimal risk that the incident poses a significant risk of harm.

Protected Health Information (PHI) (cont.)

- **Health Information Technology for Economic and Clinical Health (HITECH) Act (2009)**: Provides data breach notification and reporting requirements
  - **Individual:** Within 60 days of discovery if there significant risk of harm to individual
  - **HHS:** Breach affecting >500 individuals
  - **Media:** Breach affects >500 individuals in one jurisdiction
- State healthcare privacy/security laws, overlay with general privacy/security (GLBA), Health Information Trust Alliance (HITRUST) - Common Security Framework (CSF) (derived from ISO 27001)

Personal Financial Information

- **Gramm-Leach-Bliley Act (GLBA):** Requires financial institutions to (1) store personal financial information in a secure manner, (2) explain their information-sharing practices to their customers, and (3) allow consumers to opt-out of sharing some personal financial information.
  - Enforced by the Federal Trade Commission (FTC)
- **Fair and Accurate Credit Transactions Act (FACTA):** Requires financial institutions and creditors with covered accounts to take measures to protect consumer account information from identity theft
  - Disposal Rule – Requires companies that collect consumer information for a business purpose to reasonably dispose of that information in a way that prevents unauthorized access and misuse of the data.
    - FTC may enforce civil penalty of up to **$2,500** per violation

Payment Card Data

- Payment Card Industry Data Security Standards (PCI DSS) apply to entities that store, process, and/or transmit cardholder data.
  - A common set of industry tools and measurements to help ensure the safe handling of sensitive information
  - Covers technical and operational system components included in or connected to cardholder data
  - Provides an actionable framework for developing a robust account data security process - including preventing, detecting and reacting to security incidents
  - Version 3.2.1 released May 2018

- Payment Application DSS (PA-DSS) apply to software developers and integrators of payment applications that store, process, or transmit cardholder data as part of authorization or settlement when these applications are sold, distributed, or licensed to third parties.

FISMA

FISMA

- Enacted in 2002, amended in 2014.
- Ensures the security of fed government information systems
- Enforced by OMB and DHS (as of 2014)
- Applies to both information and info systems
- Incorporates standards developed by NIST
- Focused on risk management
  - Determine risk tolerance
  - ID and assess, respond to, and monitor risk
- What does it require?
  - An Information Security Plan
  - Annual independent evaluation of security program
  - “Baseline security controls” through a combination of managerial, operational and technical measures

FISMA (cont.)

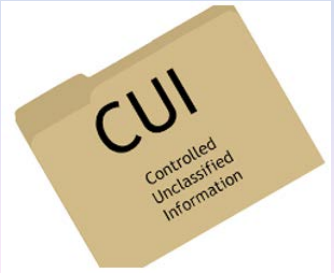
- Recent expansion to companies – over last 5-7 years
  - Applies where private company acts “on behalf of” government agency
  - Enforced through solicitation and procurement processes
- Agencies responsible for protection of “information systems used or operated . . . by a contractor of an agency or other organization on behalf of an agency.”

  => Flows down to contractors.

Controlled Unclassified Information (CUI)

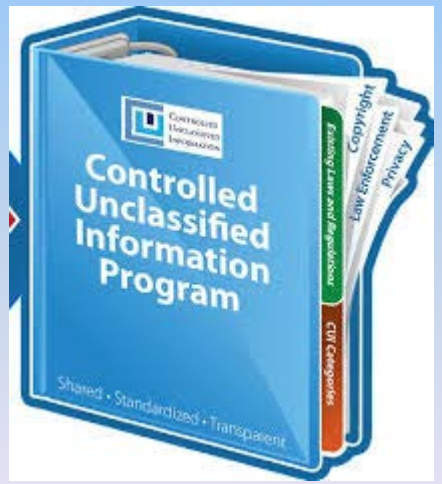
Controlled Unclassified Information (CUI)

- What is it?
  - E.O. 13556 (2010) directed the National Archives and Records Administration (NARA) to "develop a uniform program for managing information that requires safeguarding or dissemination controls pursuant to and consistent with **law**, **regulation**, and **government-wide policy**."
  - EO 13556 developed from 2009 Report from CUI Task Force led by DHS and DOJ.
  - To address inefficient and confusing patchwork system used to protect sensitive but unclassified information.
  - NARA established the program through notice and comment rulemaking: 32 CFR 2002, effective November 14, 2016.



Controlled Unclassified Information (CUI)

- Information that meets the CUI standard (law, regulation, or government-wide policy) is approved by NARA as a category or subcategory of CUI and reflected in the CUI Registry.
- New categories of CUI can be created through law, regulation, or government-wide policy; NARA can recognize "provisional categories."
- CUI Registry is available at: https://www.archives.gov/cui/registry/category-list
- Current Categories Include:
  - Controlled Technical Information
  - Export Control information
  - Law Enforcement Sensitive Information
  - Privacy information (including, e.g., PII and health information)
  - Procurement and Acquisition information
  - Proprietary Business Information



National Archives and Records Administration (NARA) CUI Final Rule

- Core Features of the Rule:
  - Establishes two types of CUI:
    - **CUI Basic**. The default CUI standard; sharing must be in furtherance of a lawful government purpose and not otherwise prohibited by law, amongst other requirements.
    - **CUI Specified**. The law, regulation, or government-wide policy articulates different sharing and safeguarding standards. CUI Registry should reflect these specific requirements.
    - Where a Specified authority is silent on a safeguarding standard, it defaults to the Basic standard.
  - Establishes marking standards (No more FOUO or SBU)
    - Must be marked as CUI, and possibly the subcategory, prior to dissemination. Exceptions and waivers applicable for legacy material.
  - Establishes standards and process for decontrolling
  - Provisions related to Information Sharing Agreements, Limited Dissemination Controls, and consequences for misuse.

National Institute of Standards and Technology (NIST)

NIST

- Not the law, but might as well be (think of the ABA Model Rules)
  - Non-regulatory agency of the Department of Commerce
    - Originated as Bureau of Standards in 1901 – Congressional authority "to fix the standards of weights and measures" (Article I, Section 8, Paragraph 5)
    - Mission: "Promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life"
  - Supporting docs and guidance for FISMA, FAR, DFARS, etc.

NIST SP 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations

- Catalog of security and privacy controls for **federal information systems** (except national security systems, which are subject to controls in CNSS Instruction (CNSSI) No. 1253)
  - Covers systems operated *on behalf of* an agency by a contractor
  - Over 150 Moderate Impact Controls (Rev. 4) (also includes controls for "low" and "high")
- SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations* - Provides specific guidelines for periodically assessing security controls
- Draft Rev. 5 (Aug. 2017) adds 2 privacy control families
  - Final publication expected Summer 2019

NIST SP 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations

18 Security Control Families	
Access Control	Media Protection
Awareness and Training	Physical and Environmental Protection
Audit and Accountability	Planning
Security Assessment and Authorization	Personnel Security
Configuration Management	Risk Assessment
Contingency Planning	System and Services Acquisition
Identification and Authentication	System and Communications Protection
Incident Response	System and Information Integrity
Maintenance	Program Management

NIST SP 800-171 – Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

- Protects Controlled Unclassified Information (CUI) for **non-federal information systems**
- Includes "basic" and "derived" requirements
  - Basic requirements originate from FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*
  - Derived requirements come from NIST SP 800-53
- NIST SP 800-171 is tailored to non-federal systems and does not include the unique federal controls in NIST SP 800-53
- Rev. 1 (Dec. 2016) added control for System Security Plan
  - Rev. 1 last updated June of 2018 with an appendix containing additional discussion on each CUI requirement
  - Rev. 2 expected very soon

NIST SP 800-171 – Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

14 Security Control Families	
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

NIST SP 800-171 – Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

- NIST MEP Handbook 162, “Cybersecurity Self-Assessment Handbook for Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements” (Nov. 20, 2017)
  - Intended for “small manufacturers”
  - Assessment questions related to NIST SP 800-171 security requirements
- NIST SP 800-171A, “Assessing Security Requirements for Controlled Unclassified Information” (June 13, 2018)
  - Assessment procedures for all security requirements in NIST SP 800-171
  - Mapping tables and guidance in Appendices

FAR and DFARS Clauses

FAR 52.204-21: Basic Safeguarding of Covered Contractor Information Systems

- Protects **"Federal Contract Information" (FCI)**
  - FCI is "information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government"
  - Excludes publicly available information or "simple transactional information, such as necessary to process payments"
- Contractor information systems that process, store, or transmit FCI are subject to **15 basic security requirements** from NIST SP 800-171
- Flow-down: All subcontracts (except for COTS) where the subcontractor may have FCI "residing in or transiting through its information system"
- No requirement for contractor to report incidents

DFARS 252.204-7012: Safeguarding Covered Defense Information (CDI)

- DoD contractors must provide "adequate security" for **"covered defense information" (CDI)**
  - CDI is unclassified controlled technical information, further described at http://www.archives.gov/cui/registry/category-list.html, which is marked and provided by the Government to the contractor, or otherwise generated/accessed by the contractor, for contract performance
- **"Adequate security"** means compliance with the NIST SP 800-171 standards, except:
  - May need additional controls if dictated by a risk assessment (DFARS 252.204-7012(b)(3))
  - There are separate standards for cloud computing services (*see* DFARS 252.239-7010) and for information systems operated "on behalf of" the Government (*see* NIST SP 800-53)

DFARS 252.204-7012: Safeguarding Covered Defense Information (CDI)

- Deadline: ASAP, but no later than **December 31, 2017**
  - Implementation means a **System Security Plan** and **Plans of Action**
  - Note: May be used as an evaluation factor and in source selection
- Flow-down: All subcontracts involving CDI or "operationally critical support"
  - If using an external cloud service provider, vendor must comply with the FedRAMP Moderate baseline
- Incident Reporting: "Rapidly report" (within 72 hours of discovery)
- Cyber incident requirements:
  - Submit malicious software you discover to DoD Cyber Crime Center
  - Preserve media of affected systems for at least 90 days, and share it with DoD if it conducts a damage assessment
  - Comply with DoD requests for access to additional information or equipment necessary for forensic analysis

DoD FAQs

- Revised version published April 2018 (*dodprocurementtoolbox.com*)
- No specified format for SSP
  - Agencies "should not intrude into the operations or management of the contractor's internal IT system by specifying the content and format of the system security plan and plans of action…" (FAQ 50)
- No need for adjudication where security control is N/A – controls deemed not applicable need not be adjudicated "[w]hen the contractor's policy, process, etc., does not allow the circumstances addressed in the NIST SP 800-171." (FAQ 62)
- DoD to mark CDI – DoD will be responsible for marking or identifying covered defense information "provided to the contractor by the Government." (FAQ 6)
- Prime contractor "responsible for safeguarding of [CDI] throughout its entire supply chain" (FAQ 19)
  - Recommended that prime "minimize the flow down of information requiring protection" (FAQ 8)

DoD Guidance

- *Implementation of DFARS Clause 252.204-7012* (September 2017)
  - DoD will not recognize third party assessments; DoD will not certify compliance
  - Elements of SSP may be required as part of proposal and incorporated into contract; compliance may be reviewed during source selection
- *Audit of the Protection of DoD Information Maintained on Contractor Systems and Networks* (June 2018)
  - DoD IG audit to "determine whether DoD contractors have security controls in place to protect the DoD [CUI] maintained on their systems and networks from internal and external cyber threats"
- *Guidance for Assessing Compliance of and Enhancing Protections for Contractor's Internal Unclassified Information System; DoD Guidance for Reviewing SSPs and NIST SP 800-171 Security Requirements Not Yet Implemented* (November 2018)
  - Pre and Post-award considerations
  - Contemplates on-site assessments
  - Impact associated with security control not implemented

DoD Guidance

- *Strengthening Contract Requirements Language for Cybersecurity in the Defense Industrial Base* (Dec. 2018)
  - Sample SOW for requesting SSPs and Plans of Action as a contract deliverable
  - Sample SOW for requesting the identification, tracking, restricted flow down of CDI, and contractor's record of Tier 1 Level suppliers who receive or develop CDI
- *Addressing Cybersecurity Oversight as Part of a Contractor's Purchasing System Review* (Jan. 2019); DCMA to review for:
  - Compliance with contractual DoD requirements for marking and distribution statements on CUI flow down
  - Compliance of Tier 1 Level suppliers with DFARS clause and NIST 800-171
- *Strategically Implementing Cybersecurity Contract Clauses* (Feb. 2019)
  - Requests recommendations for efficient assessment of cybersecurity readiness

The Cloud

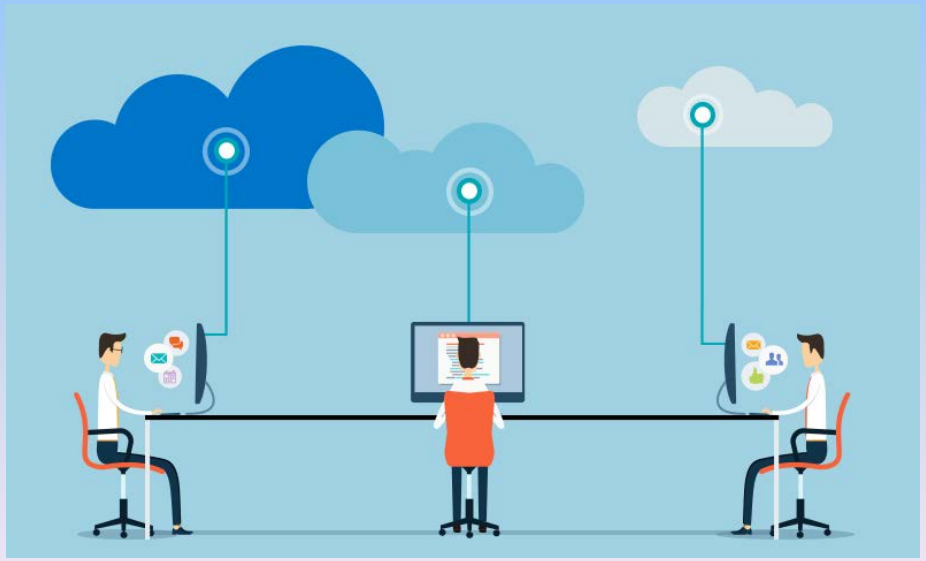
What is Cloud Computing?

- A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction

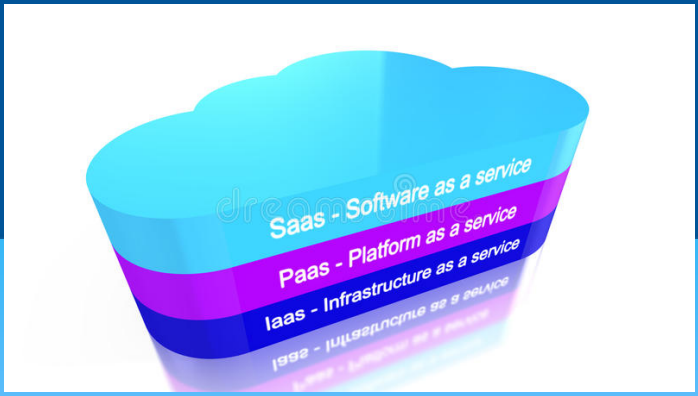
  -NIST Special Publication 800-145, The NIST Definition of Cloud Computing (September 2011).

- A style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service using Internet technologies.

  - Gartner Group



Categories of Cloud Computing



- 3 different service models for cloud products:
  - Software as a Service (SaaS) –
    - consumer uses the provider's applications running on a cloud infrastructure
    - Consumer does not manage or control the underlying cloud infrastructure.
  - Platform as a Service (PaaS) –
    - consumer uses the cloud provider's platform to deploy its own applications
    - Consumer controls the applications, but not the underlying platform.
  - Infrastructure as a Service (IaaS) –
    - consumer uses the provider's infrastructure to operate both its applications and its own platform.

FedRamp: Historical Context & Overview

The Need

Agencies were reluctant to adopt cloud computing because of security fears

The Goals

Ensure the use of cloud services protects federal information

Enable reuse across the federal government wherever possible to save money and time

The Product

A unified security framework (templates + control set) for Agencies to comply with FISMA for cloud technologies (SaaS, PaaS, IaaS) at the unclassified low, moderate, or high impact categories (FIPS 199).

FedRamp: Stakeholders

FedRAMP PMO

- Provide a unified process for all Agencies to follow
- Work with the JAB to prioritize vendors to achieve authorizations with an efficient review schedule
- Support CSPs and Agencies through the FedRAMP process
- Maintain secure repository of FedRAMP ATOs to enable reuse

AGENCIES

- Conduct quality risk assessments that can be reused
- Integrate the FedRAMP requirements into Agency specific policies/procedures
- Deposit ATO documents in the FedRAMP secure repository

CSPs

- Submit quality documentation and testing in support of their FedRAMP application for the Cloud Service Offering (CSO)
- Encourage customers to reuse existing ATOs for their CSO

3PAOs

- Maintain independence as part of the quality assurance process
- Provide quality assessments

FedRamp Designations

There are three “official” FedRAMP designations:

- FedRAMP Ready
- FedRAMP In Process
- FedRAMP Authorized

The FedRAMP PMO is the only entity that can classify CSOs as one of these three titles.

A listing of all CSOs that have achieved FedRAMP status can be found at https://marketplace.fedramp.gov/

FedRamp “Ready” Designation

Provides CSP with knowledge of likelihood of success

- Many CSPs begin a security authorization **unaware of gaps** within their system.
- The result is **unforeseen costs and more time** for CSPs in the authorization process.
- The **Readiness Assessment Report (RAR)** helps identify whether CSPs have a high likelihood of success in the authorization process (i.e, an authorization in less than 6 months).

FedRamp “Authorized” Designation

Available through JAB or Individual Agency

Joint Authorization Board Provisional Authority to Operate (P-ATO)

- The JAB is the primary governance and decision-making body for the FedRAMP program.
- CIOs of DoD, DHS, and GSA review CSP packages for an acceptable risk posture using a standard baseline approach.
- The JAB issues provisional authorizations (P-ATO); this is not a risk acceptance, but an assurance to Agencies that the risk posture of the system has been reviewed by DoD, DHS, and GSA and approved. Each Agency must review and issue their own ATO, which covers their Agency’s use of the cloud service.

Agency Authority to Operate (ATO)

- *Agency Initial (Sponsored) ATO:* Initial Agency reviews the CSP’s security package; Agency/CSP submits the security package & Agency ATO to the FedRAMP PMO; FedRAMP confirms the package meets FedRAMP requirements and makes security package available for Agencies to reuse.
- *Agency Leveraged ATO:* Agency reviews JAB or Initial Agency ATO security package and issues an Agency ATO; Agency sends a copy of the ATO letter to FedRAMP PMO for record keeping.

FedRamp “In Process” Designation

Indicates to Agencies that a CSP is actively working toward a FedRAMP authorization.

- **Obtaining the FedRAMP In Process designation**
  - The FedRAMP PMO must receive an email from an Agency Authorizing Official (AO) or a FedRAMP PMO approved designee stating they are actively engaging with the CSP and plan to grant an ATO that meets FedRAMP requirements within 12 months.
  - Additionally, **one** of the following must be demonstrated to the FedRAMP PMO:
    - Proof of an Agency-awarded contract and timeline (within the contract) for when a FedRAMP compliant ATO will be achieved
    - An email from the Agency AO or FedRAMP PMO approved designee stating Agency use
    - The CSO achieved the designation of FedRAMP Ready from the FedRAMP PMO
    - Involved parties complete a formal kick-off meeting with the FedRAMP PMO and Agency present
      - *Additional requirements associated with maintaining and removing a CSP from the FedRAMP Marketplace are located on www.fedramp.gov.*

DFARS Clauses: Cloud Computing

- DFARS 252.239-7009, *Representation of use of cloud computing*
  - contractors must represent whether they anticipate using cloud computing services "in the performance of any contract or subcontract" resulting from the solicitation
- DFARS 252.239-7010, *Cloud computing services*
  - applies where CSPs are used to process data ***on behalf of DoD***, as well as where DoD contracts with a CSP to host/process data in a cloud Requires compliance with DoD Cloud Computing Security Requirements Guide
  - Contains requirements for cyber incident reporting, malicious software, data preservation and access, and cyber incident damage assessment
  - contractor must maintain all Government data within the US, unless written authorization to use another location
- Both DFARS 252.239-7009 and -7010 must be included in solicitations and contracts for information technology (IT) services

DFARS Clauses: Cloud Computing

- DFARS 252.204-7012, *Safeguarding Covered Defense Information*
  - (b)(2)(ii)(D) – where contractor uses external Cloud Service Provider (CSP) to store, process, or transmit CDI
  - Contractor must require and ensure its CSP:
    - Is either approved by the FedRAMP program at the “moderate” baseline, or possesses equivalent security requirements
    - Complies with requirements regarding cyber incident reporting, malicious software, data preservation and access, and cyber incident damage assessment
  - This clause will normally not ‘flow down’ to the CSP; it is incumbent on the contractor itself to ensure compliance with clause requirements
- Note (b)(1)(i) refers to DFARS 252.239-7010 for requirements for cloud computing services

Insider Threat

What's the Big Deal?

- Reports from **2012** and **2014** found over 50% of cyberattacks were the result of insider action
  - **2016** – 31% of companies surveyed had an insider incident
  - Companies said damage caused by insiders greater than that of outsiders
- Most privileged users will access sensitive data simply out of curiosity if able
- The majority of insider crimes may be going unnoticed
- Financial losses from cybersecurity events increasing each year

Insider Threat

- A current or former employee, contractor, or business partner
  - With authorized access to an organization's network, system, data, premises, or assets
  - Who may misuse that access to damage or compromise the confidentiality, integrity, or availability of the organization's information or information systems
  - Can include outsiders that have stolen or been given valid user credentials
- May be merely negligent OR malicious/ideologically motivated

National Security Systems

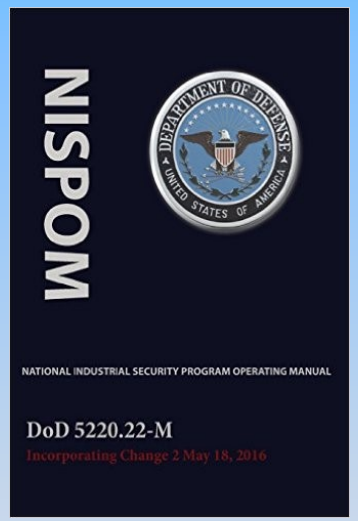
- The Committee on National Security Systems (CNSS) sets national-level Information Assurance policies, directives, instructions, operational procedures, guidance and advisories for the security of National Security Systems (NSS)
- NIST SP 800-59, *Guidelines for Identifying an Information System as a National Security System*
- CNSS Instruction (CNSSI) No. 1253 – *Security Categorization and Control Selection for National Security Systems*
  - A "companion" to NIST SP 800-53
  - Adopts FIPS 199

Efforts to Combat Insider Threats

- National Insider Threat Task Force: Interagency task force responsible for developing an executive branch insider threat detection and prevention program to be implemented by all departments and agencies.
- Security Executive Agent Directive (SEAD) 5 (May 2016): Permits agencies to collect and evaluate valuable publicly available social media information as part of vetting for national security eligibility.
- OPM launched the National Background Investigations Bureau (NBIB) on Oct. 1, 2016 to improve the security clearance process.
- Requirements specific to insider threats for contractors subject to NIST SP 800-171 and NISPOM Conforming Change 2

NISPOM Conforming Change 2

- Applies to classified information/facilities
- Contractors must establish and maintain an insider threat program to detect, deter, and mitigate insider threats
  - Designate Insider Threat Program Senior Official
  - Implement written plan
  - Training and awareness
  - User monitoring
  - Government reviews
  - Annual self-inspections



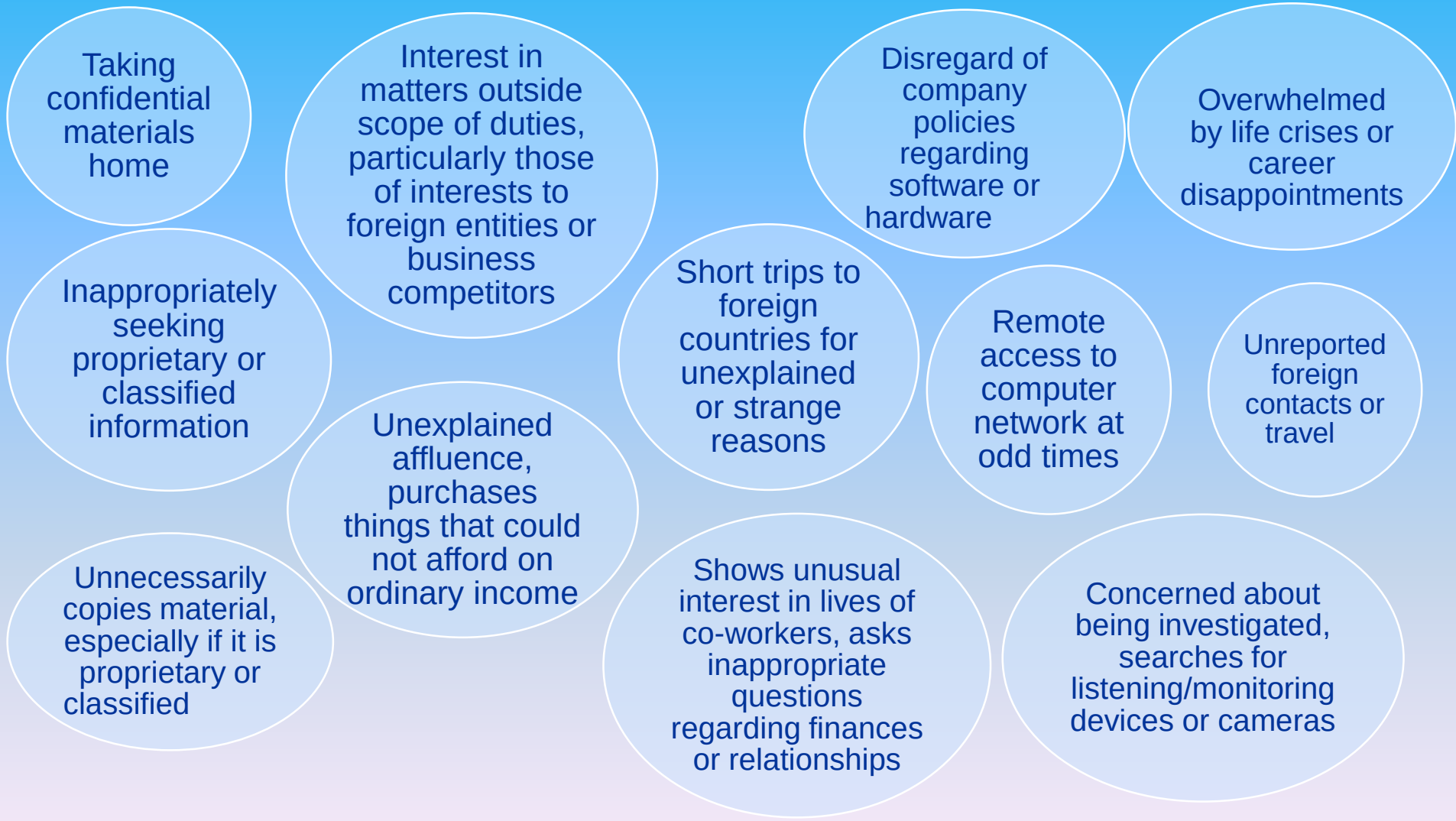
- Immediately report relevant and credible information that may be indicative of potential or actual insider threats

NISPOM Conforming Change 2

- In-house Legal, Information Security, and Human Resources must collect and share information related to 13 personnel security adjudicative guidelines:

(1) US Allegiance	(7) Alcohol Consumption
(2) Foreign Influence	(8) Drug Involvement
(3) Foreign Preference	(9) Psychological Conditions
(4) Sexual Behavior	(10) Criminal Conduct
(5) Personal Conduct	(11) Handling Protected Info.
(6) Finances	(12) Outside Activities
	(13) Use of Information Technology System

Insider Threat Behavioral Indicators



Insider Threat Personal Factors

- Greed or financial need; excessive debt
- Anger/revenge; disgruntlement
- Problems at work; lack of recognition, disagreements
- Ideology/identification; desire to help a particular cause
- Divided loyalty; allegiance to another person, company or country
- Adventure/thrill
- Vulnerability to blackmail
- Ego/self-image; “above the rules” mentality
- Ingratiation; desire to please
- Compulsive/destructive behavior; drug or alcohol abuse
- Family problems

DoD Final Rule on Insider Threat Information

- Issued October 17, 2016
- Information collected for the purpose of tracking potential “insider threats” is exempt from Privacy Act disclosure requirements
- Records collected by DOD’s Insider Threat Management and Analysis Center (“DITMAC”) intended to bring together all details on potential insider threats from various DOD agencies and contractors
- Under Privacy Act, personally identifiable information collected by federal agencies is required to be kept to a minimum, and the details of any personal information held must be made available to affected individuals upon request

DoD Final Rule on Insider Threat Information

Final rule exempts DoD from usual requirements to:

- Limit the information it holds on individuals within its insider threat system
- Make sure all records are maintained in a way meant to “assure fairness” to their subject
- Collect information directly from subjects, even where practical to do so
- Allow individuals to access any information held on them within the system
- Notify affected individuals when their information is used by another agency or is made available as a matter of legal process
- Allow any review or civil action in relation to those records

Comments on final rule raised concerns:

- Definition of “insider threat” used for DITMAC is so broad as to allow for “essentially unbounded” data collection
- Sensitive information about individuals could be damaging to individuals if caught up in a government data breach, like last year’s Office of Personnel Management hack
- Use of unverified data in DITMAC has the potential to allow for unfair bias
- May create a “climate of suspicion and secrecy” that would dissuade capable people from serving within the DOD or the defense

Insider Threat Best Practices

- Know your business and your employees
- Approach the threat holistically
- Create and enforce clear policies and procedures
- Ensure concise and coherent documentation, consistent enforcement, and periodic employee training on these policies
- Ensure the punishment fits the crime
- Periodically review and update your Insider Threat Program

Best Practices

- **Remember: Compliance ≠ Security**
  - Know your data/systems
  - Know your employees
  - Know your obligations
  - Establish/maintain cybersecurity policies/procedures and plans
- Cybersecurity is not just an IT issue; it's a risk mitigation issue
  - Not a question of whether, but when
  - No company is "too small" to be attacked

Sheppard Mullin Privacy & Cybersecurity

Jonathan Meyer
T: 202.747.1920
jmeyer@sheppardmullin.com

Townsend Bourne
T: 202.747.2184
tbourne@sheppardmullin.com