Overview of the Cyber Legal and Regulatory Maze

Phillip R. Seckman
Michael J. McGuinn

November 10, 2016

Series Overview & Objectives

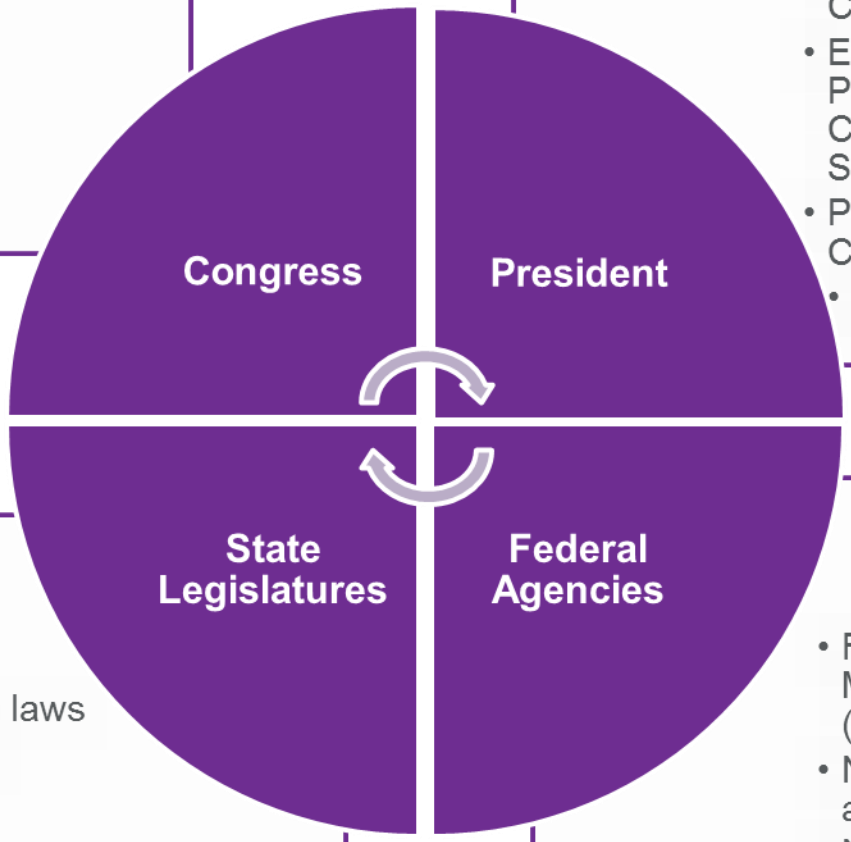
- Summarize the broad range of sources of cybersecurity requirements
  - Begin with a high-level overview
  - Subsequent sessions probe specific requirements in greater depth
- Provide practical guidance on how to address these requirements as part of an effective compliance program
- Help craft a high-level outline for such a program:
  - Begin to address the applicability of those requirements to your organization
  - Be able to conduct a basic, baseline assessment of organization's compliance
  - Gain basic understanding of how to parlay the results of such a gap analysis into an effective compliance program

Why is Cybersecurity So Important?

- Malicious cyber actors are out there
  - Foreign state-sponsored espionage
  - Cyber criminals
  - “Hacktivists”
  - Internal threats
- Breaches occur frequently
- Serious consequences and legal ramifications
  - Theft of personal/financial data or intellectual property
  - Disruption/denial of services
  - Reporting obligations under state and federal law and potential liability
- All federal contractors now face baseline cybersecurity safeguarding requirements, and that is only going to expand

Key Players Regulating Cybersecurity

- FISMA
- HIPAA
- Privacy Act
- CISA



- Executive Order 13636 – Improving Critical Infrastructure Cybersecurity
- Executive Order 13691 – Promoting Private Sector Cybersecurity Information Sharing
- PPD 41 – U.S. Cyber Incident Coordination
- Commission on Enhancing National Cybersecurity

- 47 breach notification laws
- Possibility of Federal Preemption

- FTC, FCC, DOJ Office of Management and Budget ("OMB")
- National Institute of Standards and Technology ("NIST")
- National Archives and Records Administration ("NARA")
- Contracting agencies

Sources of Cybersecurity Requirements

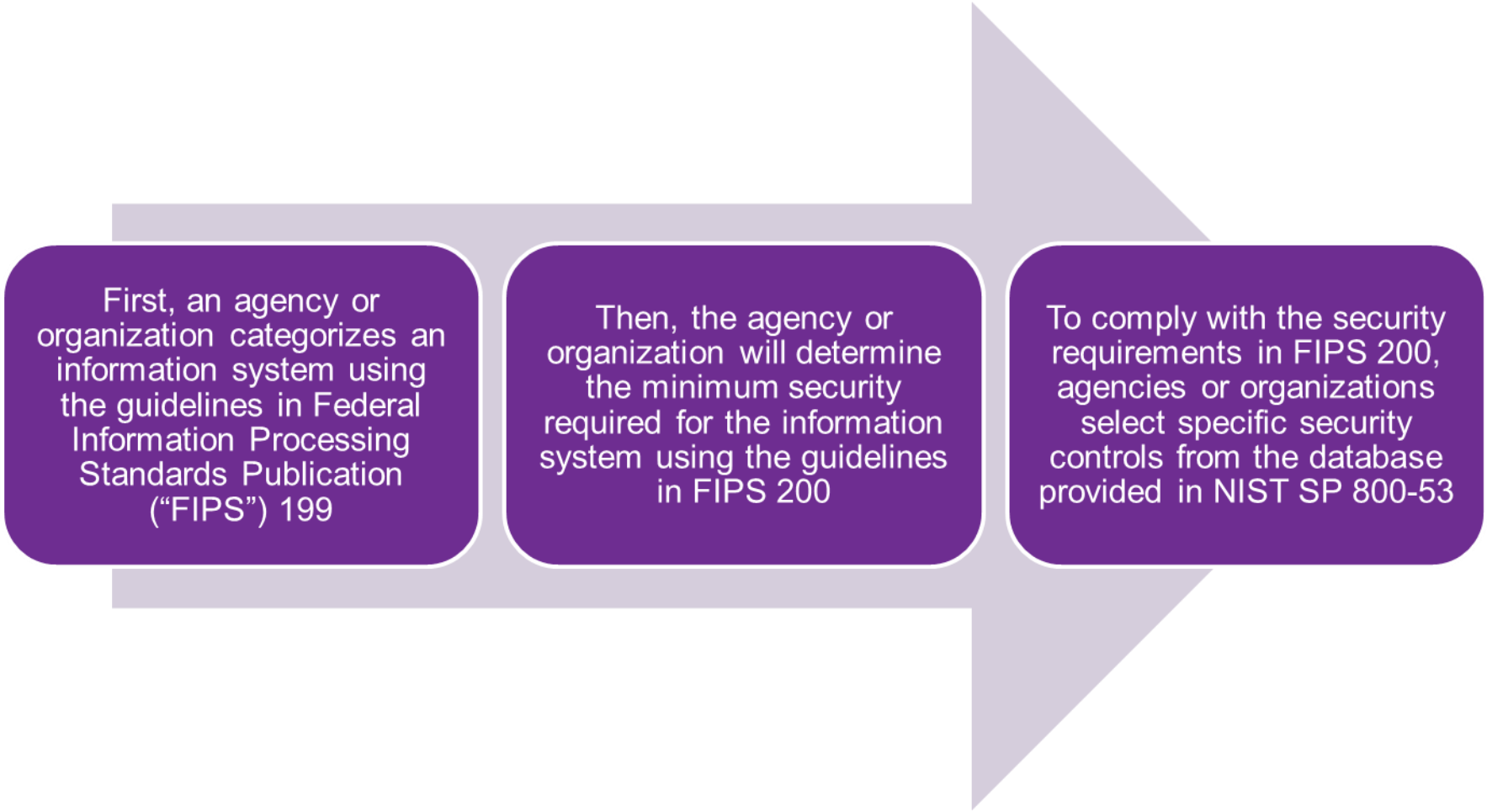
- Statutes (Federal and State)
- Executive Orders
- Regulations
- Government-wide policies
- Contract clauses
- Industry Standards & best practices
- Company policies & procedures
- International

Federal Statutes: Overview of Federal Information Systems

- More than 50 different statutes addressing cybersecurity in some way
  - HIPAA (42 U.S.C. § 1320d-2(d)) (healthcare data)
  - Privacy Act (5 U.S.C. § 552a) (federal systems of records)

- Federal Information Security Management Act of 2002
  - Codified at 44 U.S.C. § 3551-58
  - Primary cybersecurity legal authority applying to the federal government
  - Requires agencies to develop information security programs implementing NIST and OMB standards

Federal Statutes: FISMA Compliance Process



FISMA Requirements for Contractors

- Contractual requirements
- Implement controls from NIST SP 800-53
  - 17 control families
- Risk Management Framework - NIST SP 800-39
  - Categorize → Select Security Controls → Implement Security Controls → Assess → Authorize → Monitor
- Authorization to Operate ("ATO") Package

Regulations: FISMA Requirements for Contractors (*cont'd*)

Federal-wide Regulatory Requirements

- FAR § 7.103(w) - Requires agency heads to ensure compliance with FISMA and related guidance when acquiring information technology
- FAR § 39.101 – Requires agencies to follow OMB Circular A-130 and NIST publications
- OMB Circular A-130 – Issued in 1996 and establishes very general guidelines

Agency-Specific Regulatory Requirements

- GSAR § 552.239-70 and -71 (GSA)
- HHSAR 352.239-72 (HHS)
- DOSAR § 652.239-70 and -71 (State Department)
- NFS § 1852.204-76 (NASA)
- HUD, Nuclear Regulatory Commission, Dep't of Transportation, and VA also have regulations
- Generally require FISMA authorization to operate process prior to contract performance

Federal Statutes: Cybersecurity Information Sharing Act

- CISA was enacted at the end of 2015 and clarifies certain uncertainties regarding the propriety of obtaining and sharing threat information between private entities and with the federal government.
- Establishes a process lead by the Department of Homeland Security for sharing and receiving cybersecurity threat information by the federal government, including real-time-sharing of cyber threat indicators and sharing of classified threat intelligence information to properly cleared individuals
- Affords specific liability protection for monitoring networks for cybersecurity information and sharing or receiving threat information in accordance with the Act.
- Required DOJ and DHS to issue guidance which was finalized in June 2016.

Federal Statutes: FTC Enforcement & FCC Fines

- FTC has long charged companies with unfair trade practices for failure to protect customers from a data security breach
  - *FTC v. Wyndham Worldwide Corp. et al*
  - Section 5 prohibition against "unfair or deceptive practices" may apply to data breach scenarios

- FCC enforcement actions for negligent cybersecurity practices
  - YourTel America and TerraCom Inc. fined $10 million (Oct. 2014)
  - AT&T reached $25 million settlement (Apr. 2015)
  - FCC Chairman Wheeler – the "Commission will exercise its full authority against companies that fail to safeguard the personal information of their customers."

Executive Orders: Protecting Controlled Unclassified Information

- National Archives and Records Administration (“NARA”)
  - Executive agency in charge of CUI (E.O. 13556)
- Final Federal CUI Regulation issued Sept. 14, 2016
  - 81 Fed. Reg. 63324
  - Government-wide policy for safeguarding CUI
  - Establishes CUI Program and creates CUI Registry
  - Final rule strives to clarify and obtain uniform treatment of CUI across the federal government
  - Pending FAR case will extend directive to federal contractors
- NIST SP 800-171
  - Issued in June 2015
  - Guidance on protecting CUI residing in non-federal systems

Executive Orders: “Controlled Unclassified Information”

- “Information that law, regulation or governmentwide policy requires to have safeguarding or disseminating controls, excluding classified information”
- CUI Registry – 23 categories and 82 subcategories, including:
  - Agriculture
  - Controlled Technical Information
  - Critical Infrastructure
  - Emergency Management
  - Export Control
  - Financial
  - Immigration
  - Information Systems Vulnerability
  - Intelligence
  - Law Enforcement
  - Legal
  - Nuclear
  - Patent
  - Privacy
  - Proprietary Business Information
  - SAFETY Act Information

Executive Orders: Compliance with NIST SP 800-171

- NIST SP 800-171 built on the assumption that the FIPS 199 *confidentiality* impact value for CUI is no less than *moderate*
- Two-tiered security requirements structure
  - Basic requirements – FIPS 200
  - Derived requirements – NIST SP 800-53 “moderate” baseline
- Tailors these security requirements to eliminate controls that are:
  - Uniquely federal (i.e., primarily the responsibility of the government)
  - Not directly related to protecting the confidentiality of CUI
  - Expected to be routinely satisfied by nonfederal organizations without specification
- This leaves 14 security control families and related security controls specified in NIST SP 800-171

Implementation of NIST 800-171

- Final NARA rule confirms that a future FAR clause will extend the federal CUI regulation to contractors to require implementation of at least some subset of the requirements of NIST SP 800-171 to federal contractors

- Until single FAR clause is established, federal agencies are encouraged to reference the CUI safeguarding requirements in NIST SP 800-171 in contractual requirements

- Some agencies have already begun to adopt new contract clauses implementing the controls in NIST SP 800-171 (DOD, FAR Basic Safeguarding of Covered Contractor Information Systems)

Executive Orders: NIST Cybersecurity Framework

- Voluntary framework based on existing standards, guidelines, and practices for reducing cyber risks to critical infrastructure
- Executive Order 13636 tasked NIST with developing the Framework for Improving Critical Infrastructure Cybersecurity
- Seeks to provide a common language for understanding, managing, and expressing cybersecurity risk both internally and externally
- Framework Core
  - Five Core Functions
  - Twenty-two categories under the five functions
  - Maps categories and subcategories to existing standards,

Executive Orders: Cybersecurity National Action Plan

- Executive Order Issued February 9, 2016
  - Establishes "Commission on Enhancing National Cybersecurity"
  - Creates a new Federal Chief Information Security Officer
  - Launches a National Cybersecurity Awareness Campaign
  - Invests over $19 billion in cybersecurity as part of President's FY2017 proposed budget

- Commission will make recommendations on actions to be taken over the next decade over a range of dimensions, to include bolstering partnerships between public and private sectors.
  - NIST has issued an RFI to assist the CENC on its information gathering.
  - Likely source of eventual further procurement reforms, but these are a long way off

Regulations: Protecting “Federal Contract Information”

- FAR Basic Safeguarding Rule, Effective June 15, 2016 (81 Fed. Reg. 30439)
  - Establishes new FAR Clause, 52.204-21, Basic Safeguarding of Covered Contractor Information Systems (June 2016)
  - Intended to establish a basic level of safeguarding for all federal government contractors
  - Applies to contractor information systems that process, store, or transmit "federal contract information"
    - Non public information "that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government"
    - Intended to be read very broadly
  - Imposes 15 different security controls (though not specifically linked to SP 800-171, taken verbatim from those controls)

Regulations: Protecting "Covered Defense Information"

- DoD issued a final Network Penetration Reporting and Contracting for Cloud Services rule on October 21, 2016
  - August and December 2015 Interim rule significantly amended the structure of DoD cybersecurity requirements for contractors (80 Fed. Reg. 51739) (80 Fed. Reg. 81472)
- Final rule confirms expanded applicability of the rule, clarifies certain other aspects, and raises new questions
- Consistency across defense and civilian agencies
  - Requires implementation of NIST SP 800-171 security controls (or alternate but equally effective controls)
- Imposes continued reporting obligation

Regulations: What is “Covered Defense Information”?

- DFARS Subpart 204.73, as amended by interim rule
  - "Covered defense information” means unclassified controlled technical information or other information (as described in the [CUI Registry] that requires safeguarding or dissemination controls. . ." and is either (1) marked or identified in the contract or (2) collected, developed, received, transmitted, used, or stored by the contractor in support of the performance of the contract.
- Implementation
  - Contractors have until December 31, 2017 to implement required controls
  - Requires report to DOD CIO regarding implementation progress within 30 days of award
  - Contractors may submit requests to vary from SP 800-171 controls before or after award under the final rule

Government Wide Policy: Presidential Policy Directive 41

- U.S. Cyber Incident Coordination Policy issued July 26, 2016 seeks to enhance unity of effort within the Federal Government and strengthen synchronization between public and private sector

- Establishes five guiding principles:
  - Shared Responsibility
  - Risk-Based Response
  - Respecting Affected Entities
  - Unity of Governmental Effort
  - Enabling Restoration and Recovery

Contractual Requirements: FedRAMP

- U.S. Federal Risk and Authorization Management Program (FedRAMP)
- Government-wide program standardizing security assessment, authorization, and continuous monitoring for cloud products and services
- Cloud Service Providers must meet FedRAMP's 3-step authorization process before implementing services for federal agencies.
  - Security Assessment – based on FISMA baselines in NIST SP 800-53
  - Authorization – agency reviews a provider's security authorization package to grant authorization
  - Ongoing Assessment & Authorization – third party assessment organizations complete ongoing assessments to maintain the security authorization

Contractual Requirements: Agency Specific Requirements

- Agency level regulations & requirements lack of uniformity on requirements, specificity, and structure
  - Requirements can be lurking in agency publications incorporated by reference.
  - Merits heightened review of sections H & I.
- Many agencies have separate cybersecurity/information security requirements:
  - DOD: Security & Privacy for Computer Systems; Safeguarding of Controlled Defense Information; Supply Chain Risk; breach notification
  - DHS: Security Requirements for Unclassified Information Technology Resources; internal policies incorporated by reference; NIST controls
  - GSA: CIO IT Security Procedural Guide; IT Audit access
  - HHS: HHSAR Subpart 339.71 related to HHS information systems access; internal policies incorporated by reference; security plans
- Applicability of Internal Agency Guidance not always clear

State Statutes

- 47 states have data breach notification laws
- California Notice of Security Breach Act
  - Recently expanded covered “personal information” to include a username or email address, in combination with a password or security question and answer
- New York passed four cybersecurity bills in February 2015
  - Provide safe harbor for companies adopting heightened data security standards
- Potential preemption issue if federal data breach notification legislation is passed

Practical Tips for Compliance: Step 1 – Read Your Contracts

Understand contractual obligations

- Failure to comply may lead to termination or even False Claims Act liability
- Ensure all personnel are aware of requirements and current capabilities, sales and contracts personnel included

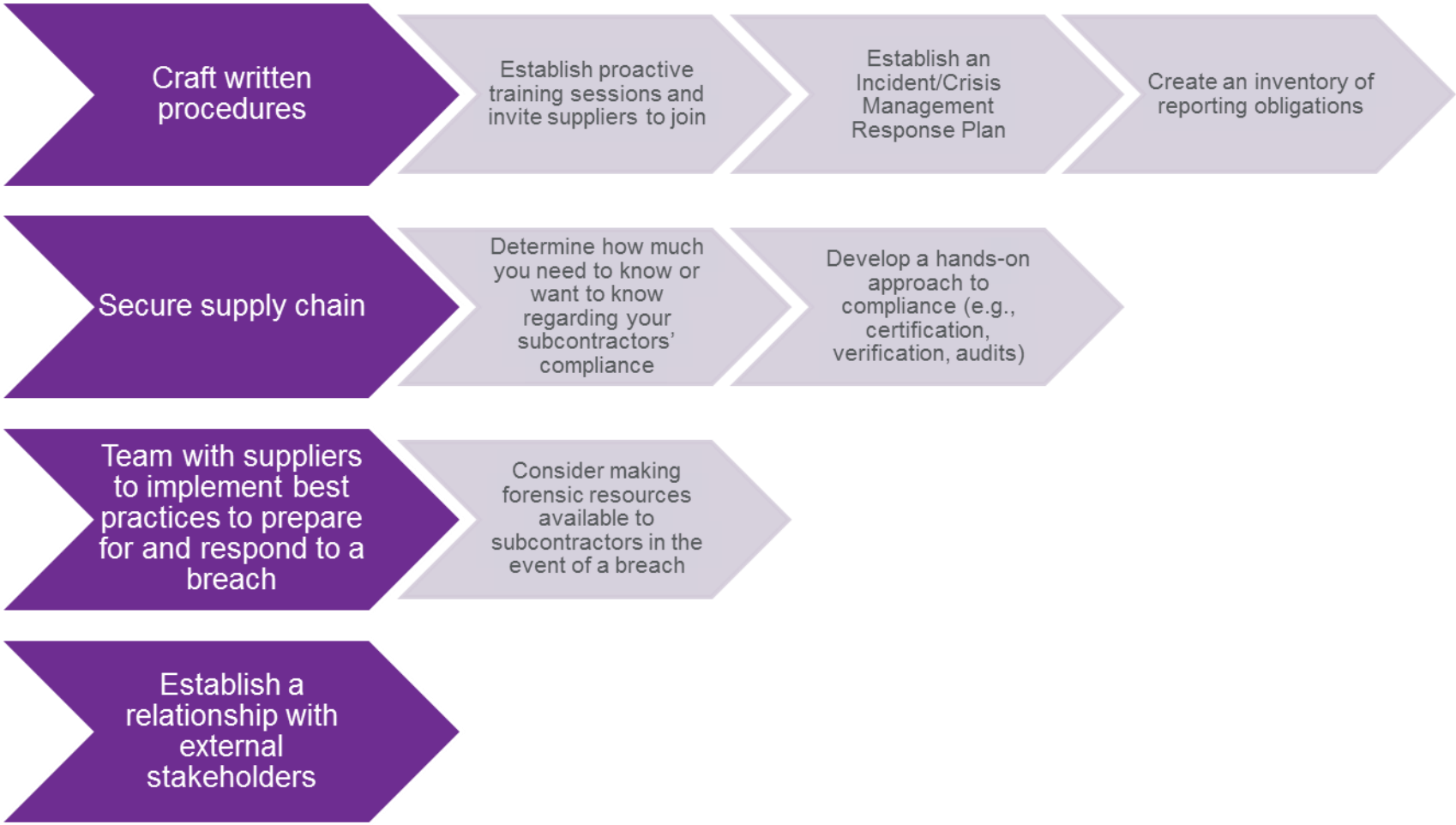
Assess flow-down requirements

- Require subcontractors to report any incident that affects data related to performance
- Some agencies, such as DoD, may require subcontractors to report incidents directly to the agency

Practical Tips for Compliance: Step 2 – Perform Gap Analysis

- How are you meeting current obligations?
- Have you identified categories of protected information?
- How are you managing your supply chain?
- Have you enacted any additional protections?
- Have you identified and assigned responsibilities in the event of a cyber incident?

Practical Tips for Compliance: Step 3 – Craft Policies and Procedures to Close Gaps



Questions?

Thank you

Dentons US LLP
1900 K Street, NW
Washington, DC 20006-1102
United States

Dentons is a global law firm driven to provide a competitive edge in an increasingly complex and interconnected world. A top 20 firm on the Acritas 2014 Global Elite Brand Index, Dentons is committed to challenging the status quo in delivering consistent and uncompromising quality in new and inventive ways. Dentons' clients now benefit from 3,000 lawyers and professionals in more than 80 locations spanning 50-plus countries. With a legacy of legal experience that dates back to 1742 and builds on the strengths of our foundational firms—Salans, Fraser Milner Casgrain (FMC), SNR Denton and McKenna Long & Aldridge—the Firm serves the local, regional and global needs of private and public clients. www.dentons.com.