DENTONS

Overview of the Cyber Legal and Regulatory Maze

Phillip R. Seckman
Erin B. Sheppard

Series Overview & Objectives

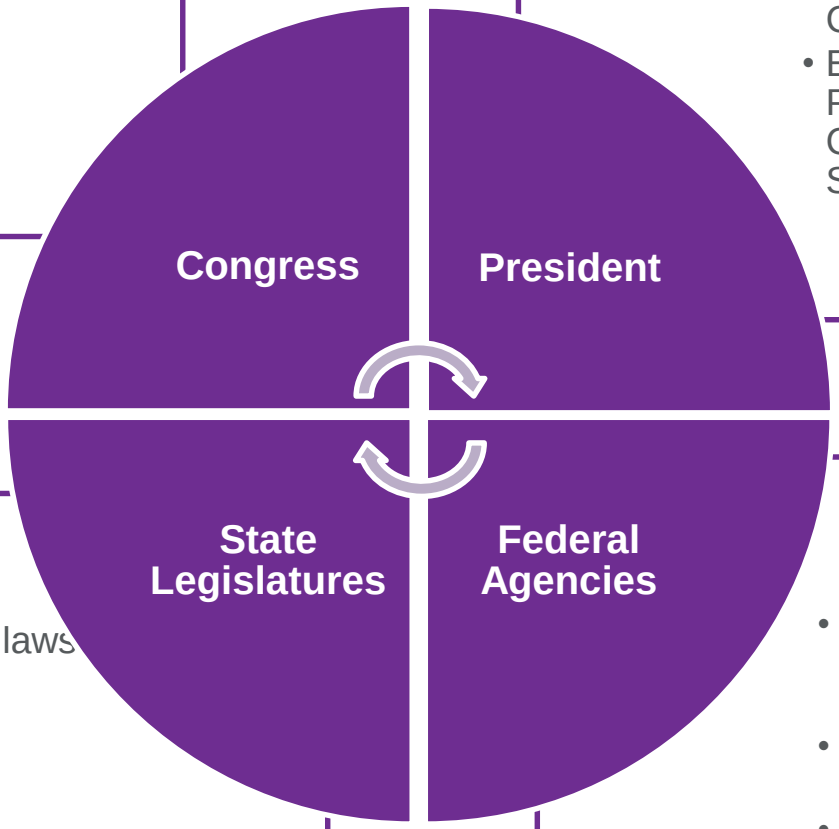
- Summarize the broad range of sources of cybersecurity requirements
  - Begin with a high-level overview
  - Subsequent sessions probe specific requirements in greater depth
- Provide practical guidance on how to address these requirements as part of an effective compliance program
- Help craft a high-level 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
  - Federal agencies reported over 67,000 incidents to the U.S. Computer Emergency Readiness Team in 2014 (up from 5,500 in 2006)
  - Defense contractors lag behind retail companies and financial institutions in cybersecurity (study by Nextgov.com using data from BitSight Technologies)
- 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

Key Players Regulating Cybersecurity

- FISMA
- HIPAA
- Privacy Act
- CISA (under Consideration)



- Executive Order 13636 – Improving Critical Infrastructure Cybersecurity
- Executive Order 13691 – Promoting Private Sector Cybersecurity Information Sharing

- 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

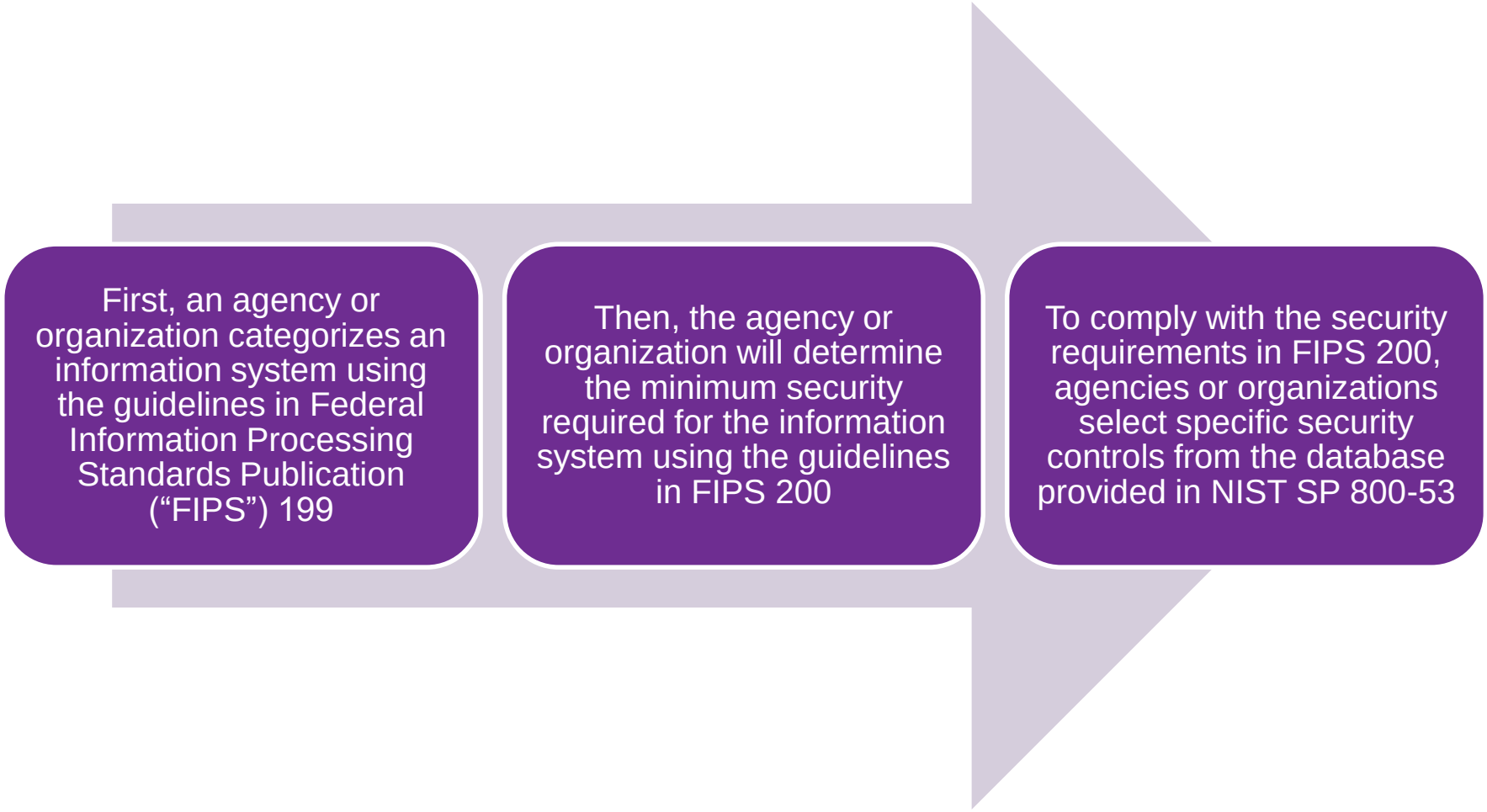
- Statutes (Federal and State)
- Executive Orders
- Regulations
- Government-wide policies
- Contract clauses
- Company policies & procedures
- Industry Standards & best practices
- State and local government
- International government

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



FIPS 199 – Security Categorization

- Categorizes information and information systems based on three security objectives:
  - **Confidentiality** – protecting against the unauthorized disclosure of information
  - **Integrity** – protecting against the unauthorized modification or destruction of information
  - **Availability** – protecting against the disruption of access to or use of information or an information system

- For each objective, the agency determines if the potential impact of a breach would be **Low**, **Moderate**, or **High**
  - $\mathbf{SC}_{\text{information system}}$ = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)}

- "High water mark" determines the overall security categorization

FIPS 200 – Minimum Security Requirements

- Specifies minimum security requirements in seventeen security related areas
  - Ex., Access Control, Incident Response, Personnel Security, Risk Assessment
- "Risk-based" process for selecting security controls necessary
  - "High water mark" categorization from FIPS 199 determines overall impact level of a system
  - Requires agencies to employ the appropriately tailored security controls from the **low**, **moderate**, and **high baselines** in NIST SP 800-53
  - Agencies may tailor these baselines as provided in NIST SP 800-53
    - "To ensure a cost-effective, risk-based approach to achieving adequate security across the organization, security control baseline tailoring activities must be coordinated with and approved by appropriate organizational officials."

NIST SP 800-53 – Security and Privacy Controls

- Provides specific controls in each of the 17 control families, as well an additional Program Management control family
- Some controls are also provided with “enhancements”
- NIST SP 800-53 identifies which controls and enhancements are required for each baseline – low, moderate, or high

FISMA Requirements for Contractors

- Contractual requirements
- Risk Management Framework - NIST SP 800-39
  - Categorize → Select Security Controls → Implement Security Controls → Assess → Authorize → Monitor
- Authorization to Operate ("ATO") Package
  - Categorization Documentation
  - System Security Plan
  - System Configuration Baseline
  - System Test and Evaluation
  - Plan of Action and Milestones
  - Detailed Risk Assessment

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: Federal Trade Commission Enforcement

- FTC has long charged companies with unfair trade practices for failure to protect customers from a data security breach
- FTC's authority to regulate corporate cybersecurity was recently upheld by the 3rd Circuit (*FTC v. Wyndham Worldwide Corp. et al*)
- Section 5 prohibition against "unfair or deceptive practices" may apply to data breach scenarios
  - If a business has made false or misleading claims about its data security
  - If a business has failed to establish reasonable security measures
- Other Statutes
  - Safeguards Rule
  - Fair Credit Reporting Act
  - Children's Online Privacy Protection Act

Federal Statutes: Federal Communications Commission Fines

- FCC issued its first fines for negligent cybersecurity practices in October 2014, fining YourTel America and TerraCom Inc. $10 million after a data breach putting up to 300,000 customers at risk
- In April 2015, the FCC reached a $25 million settlement with AT&T for a breach involving disclosure of almost 280,000 U.S. customers' names, full or partial SSNs, and protected account-related data
- 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)
- Federal CUI Regulation proposed by NARA on May 8, 2015
  - 80 Fed. Reg. 26501
  - Government-wide policy for safeguarding CUI
  - Establishes CUI Program and creates CUI Registry
- 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
  - 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

- In 2016, NARA plans to sponsor a single FAR clause that will apply the federal CUI regulation proposed in May 2015 and 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

Regulations: Protecting "Covered Defense Information"

- DoD announced an interim rule on August 26, 2015 significantly amending the structure of DoD cybersecurity requirements for contractors (80 Fed. Reg. 51739)
- Rule effective immediately, comments were due by October 26
- Rule expands applicability
  - From "unclassified controlled technical information" to "covered defense information"
  - Now applies to commercial item acquisitions and small business contractors
- Consistency across defense and civilian agencies
  - Amends DFARS § 252.204-7012 to replace the clause's previous table of security controls with NIST SP 800-171 controls
- Imposes continued reporting obligation
- Formalizes cloud computing guidance

Regulations: What is "Covered Defense Information"?

- DFARS Subpart 204.73, as amended by interim rule
  - Unclassified information
  - Provided by DoD or collected, developed, received, transmitted, used, or stored by the contractor in support of the performance of the contract
  - Falls in any of the following categories:
    - Controlled technical information
    - Critical information
    - Export Control
    - Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls

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
  - First version released on February 12, 2014
- Seeks to provide a common language for understanding, managing, and expressing cybersecurity risk both internally and externally
- Framework Core
  - Five Core Functions – Identify, Protect, Detect, Respond, Recover
  - Twenty-two categories under the five functions – ex. Asset Management, Risk Management, Access Control, Mitigation
  - Maps categories and subcategories to existing standards, such as NIST SP 800-53, COBIT 5, CCS CSC, ISA 62443-2-1:2009, ISA 62443-3-3:2013, and ISO/IEC 27001:2013

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
- Stakeholders: GAS, NIST, DHS, DoD, NSA, OMB, Federal CIO Council, and private industry
- Cloud Service Providers must meet all FedRAMP requirements before implementing services for federal agencies
- Three-Step Authorization Process:
  - 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

Industry Best Practices: DOJ Best Practices

- Department of Justice on April 29, 2015 released its “Best Practices for Victim Response and Reporting of Cyber Incidents”
- Baseline cybersecurity expectations for all organizations connected to the internet
- Separated into guidance for before, during, and after a cyber incident
  - **Before** – identify “crown jewels”; have action plan and appropriate technology in place; ensure legal counsel is familiar with cyber incident management policies
  - **During** – make initial assessment; implement measures to minimize continuing damage; record and collect information; notify law enforcement, DHS, appropriate in-house personnel, and potential victims; **DO NOT** communicate on compromised system or hack into or damage another network
  - **After** – continue monitoring network for anomalous activity; conduct a post-incident review

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

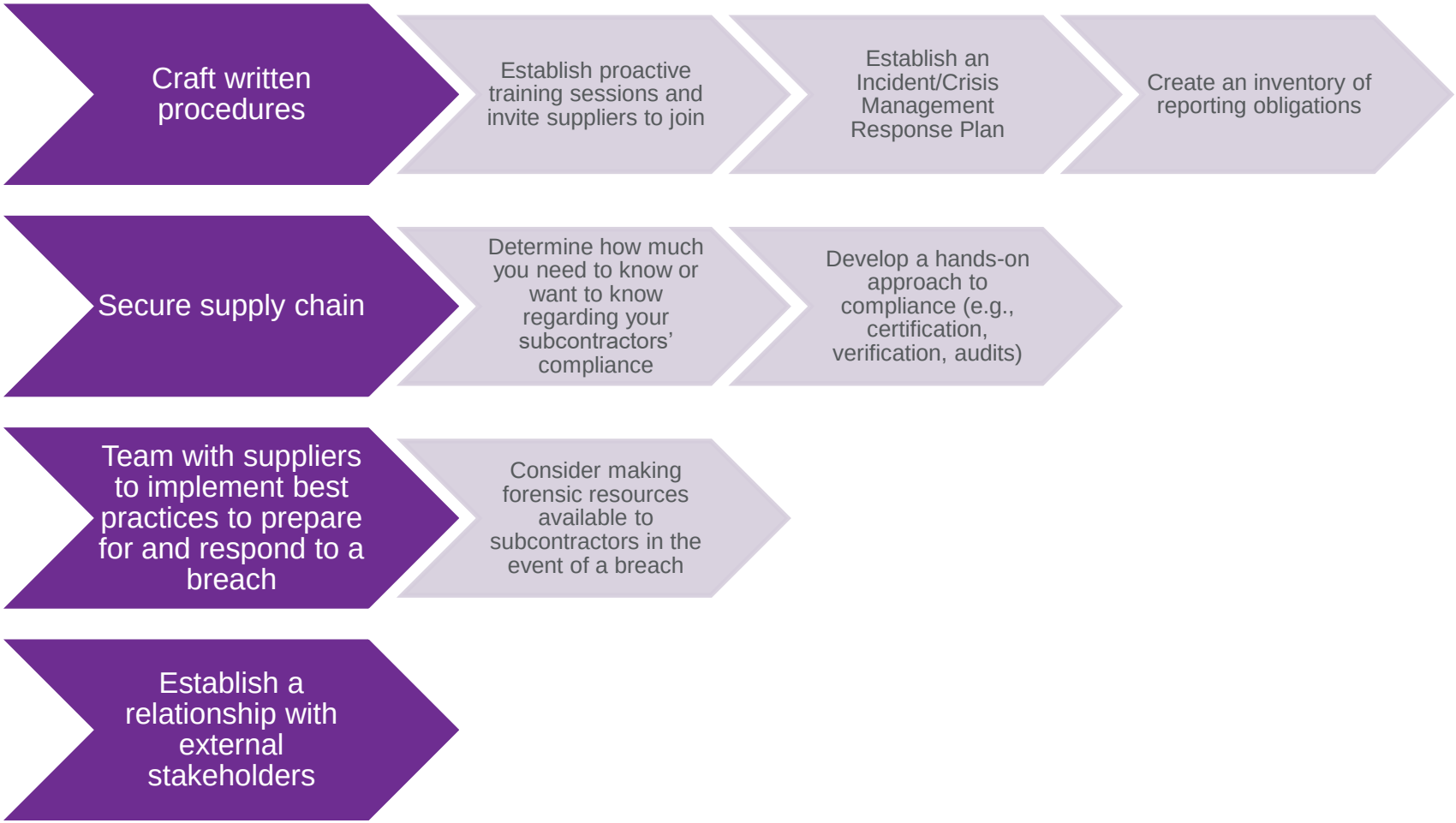
Assess flow-down requirements

- 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.

© 2015 Dentons. Dentons is a global legal practice providing client services worldwide through its member firms and affiliates. This publication is not designed to provide legal advice and you should not take, or refrain from taking, action based on its content. Please see dentons.com for Legal Notices.