Federal cybersecurity requirements

Impact to subcontractors and monitoring obligations

March 13, 2019

Building a better working world

Disclaimer

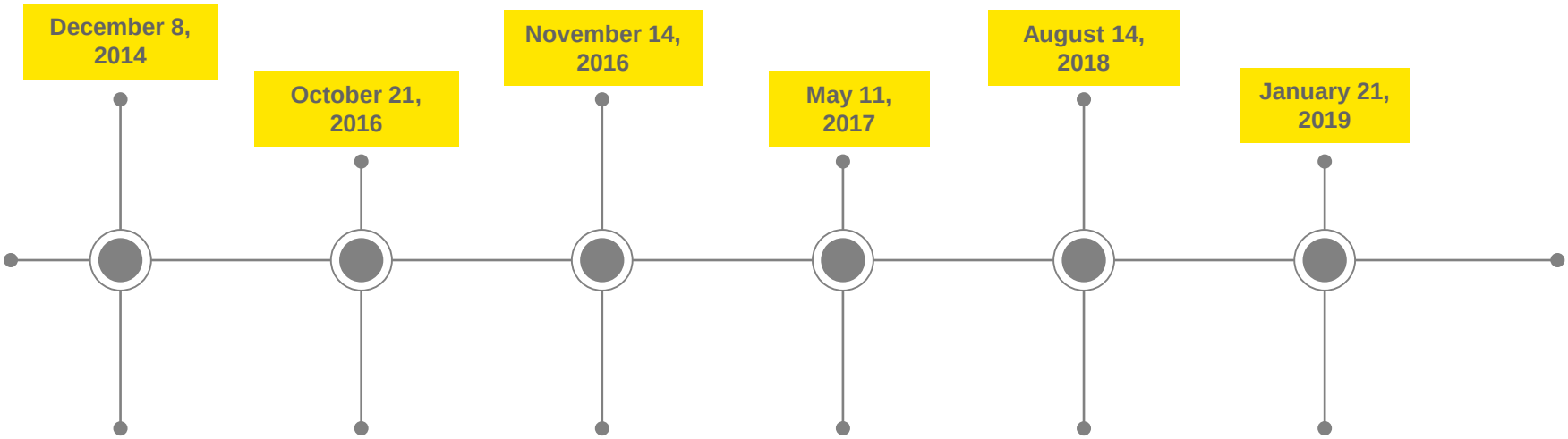
- The views expressed by the presenters are not necessarily those of Ernst & Young LLP or other members of the global EY organization.
- These slides are for educational purposes only and are not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

Agenda

1. Introductions
2. Overview of recent federal cybersecurity activity
3. Covered defense information (CDI) and Defense Federal Acquisition Regulation Supplement (DFARS) overview
4. Conducting internal assessments
5. Reporting considerations – supply chain and incident reporting
6. Anticipated cybersecurity regulations

Throughout the presentation, we have designated discussion breaks to encourage audience participation. If you have a question or comment about a topic we are discussing, please let us know!

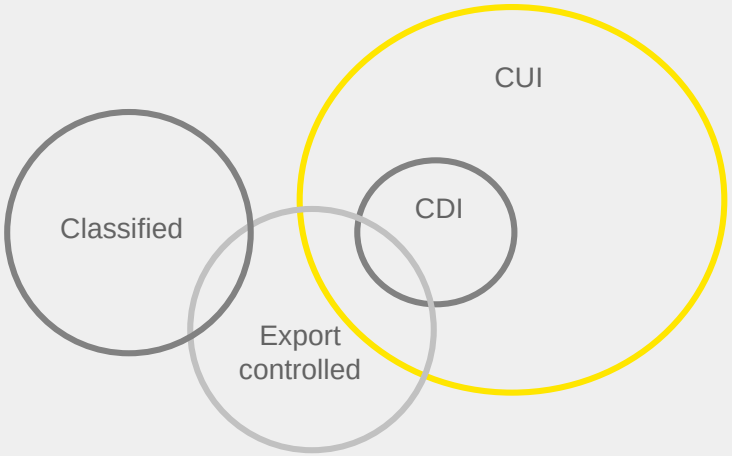
Recent history of federal cybersecurity



Controlled unclassified information

Controlled unclassified information (CUI), covered defense information (CDI) and the need to protect information on non-federal systems:

- National Archives & Records Administration CUI registry
- CDI



DFARS 252.204-7012 overview

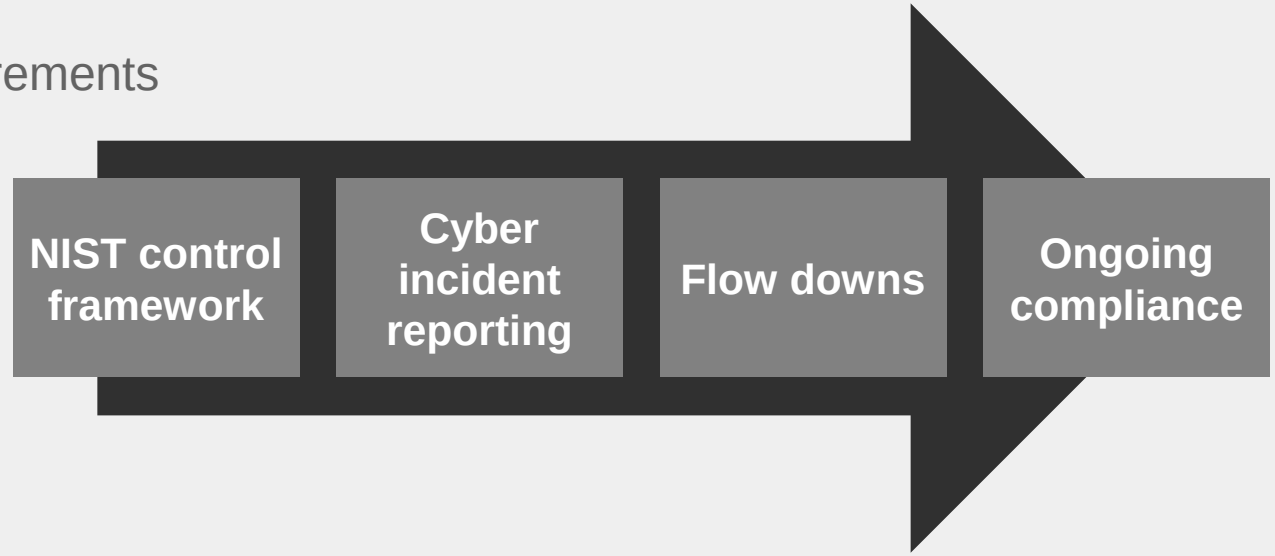
Defense Federal Acquisition Regulation Supplement (DFARS)

Safeguarding Covered Defense Information and Cyber Incident Reporting (DFARS 204.73)

Focus

The regulation focuses on the protection of covered defense information (CDI) on contractors' systems, including what constitutes this information and what steps should be taken to adequately safeguard it.

Requirements



Organizational approach

Discussion point

Applicability assessment

Identification of clause and information

1. Contractors must assess when and how the clause applies.
2. Individuals in areas across the company must understand and communicate what the DFARS clause requires contract by contract.
3. Utilize existing contract management tools and systems.
4. Awareness must be maintained throughout the project life cycle

Ongoing compliance
Control testing and validation

As required by the “adequate security” component of the clause and detailed in NIST SP 800-171 requirements, cybersecurity controls must be continuously assessed.

3.12.1	► “Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.”
3.12.3	► “Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.”

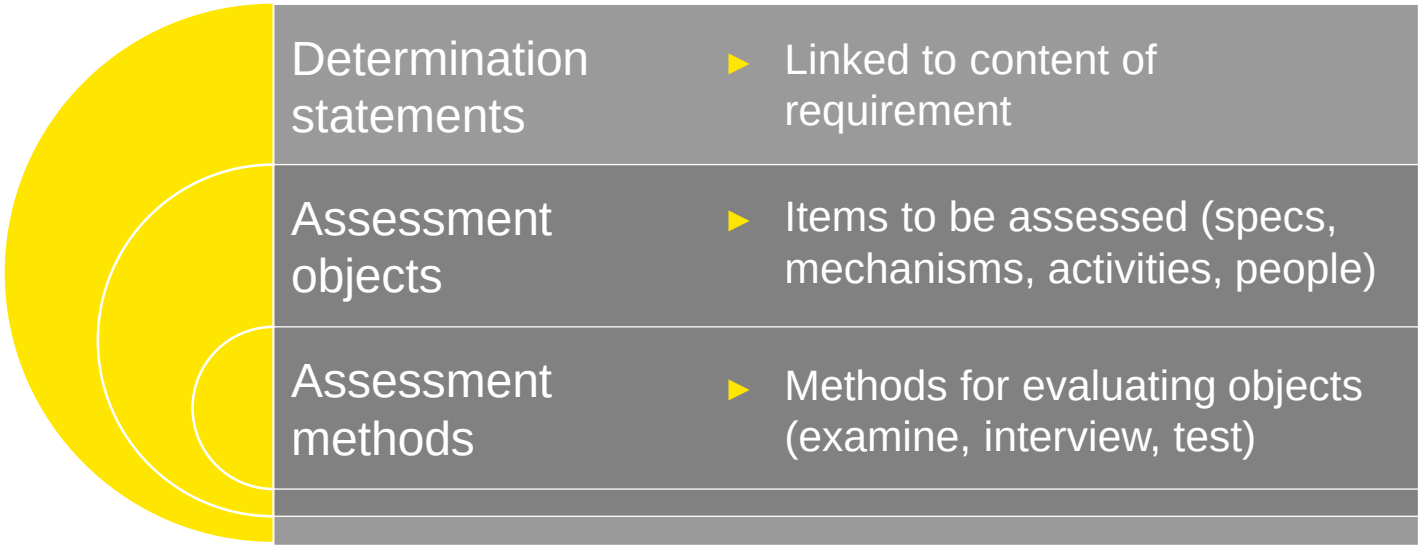
Contractors should establish a control selection and testing plan to validate activities and identify areas for enhancement through a comparative analysis against the requirements of DFARS 252.204-7012, including subcontractor oversight, incident reporting, and policies and procedures. Potential actions could include:

- Developing a method for quickly identifying in-scope contracts
- Maintaining an inventory of covered systems and IT assets
- Assign roles and responsibilities
- Maintain an inventory of tools and programs applicable to the NIST SP 800-171 controls
- Maintain control descriptions
- Maintain policies, procedures and trainings

NIST Special Publication 800-171 assessments

NIST Special Publication 800-171A Assessing Security Requirements for Controlled Unclassified Information

- Provides a methodology and procedures to determine if security safeguards are implemented correctly, operating as intended and satisfy CUI requirements



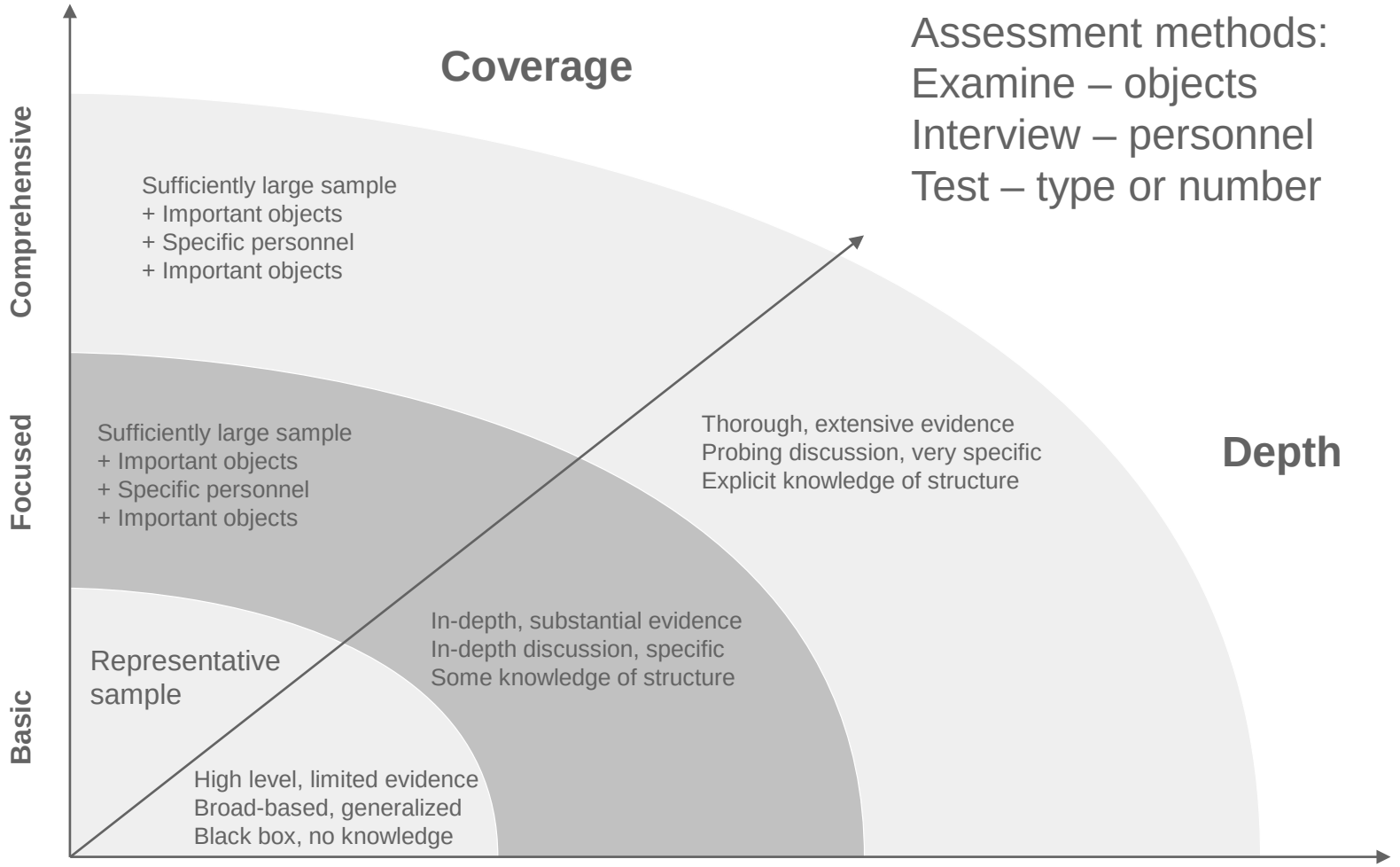
Source: *NIST Special Publication 800-171A Assessing Security Requirements for Controlled Unclassified Information*, National Institute of Standards and Technology, June 2018.

NIST Special Publication 800-171 assessments

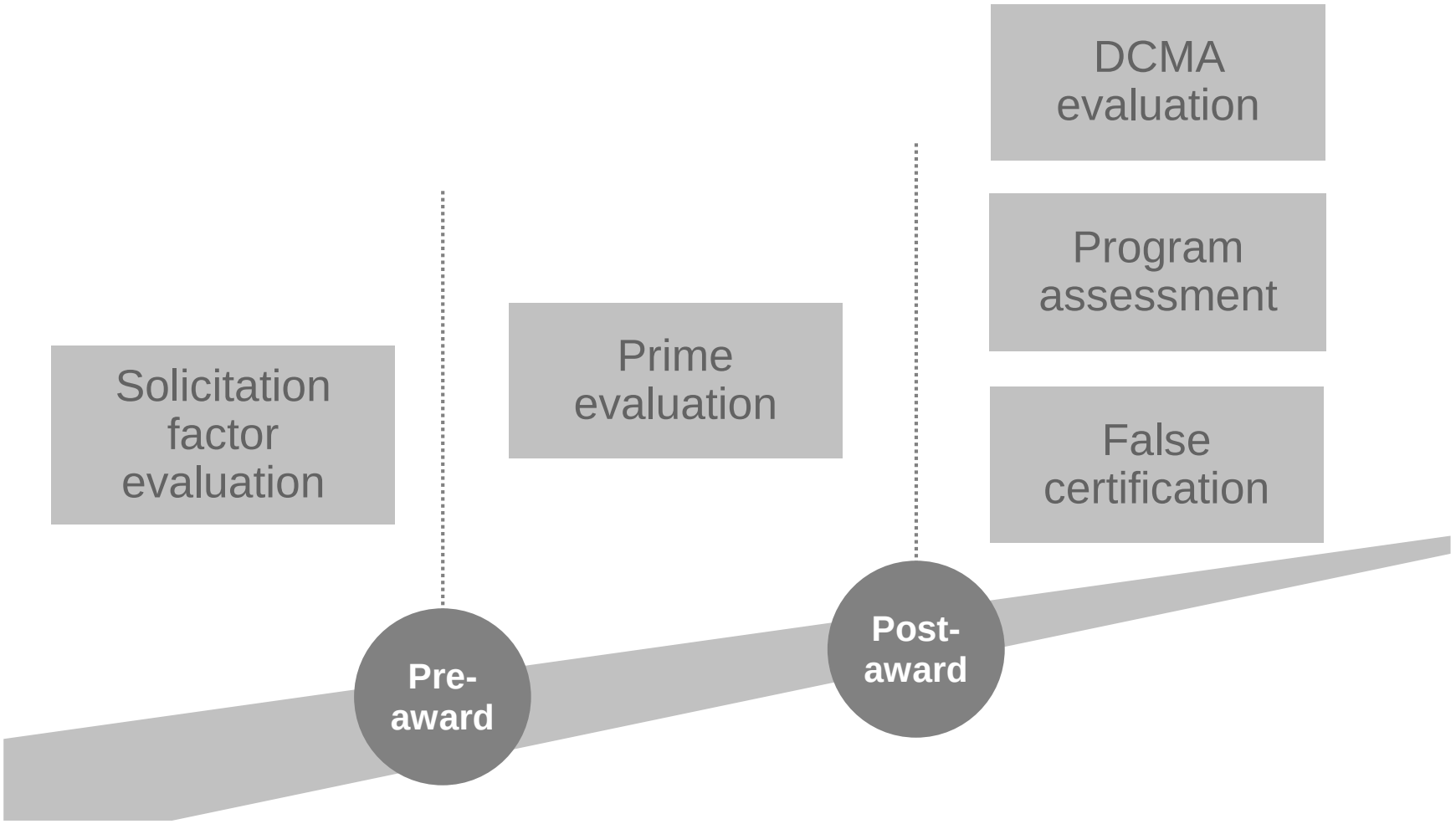
3.1.4	**Security requirement** Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	
	Assessment objective Determine if:	
	3.1.4.[a]	The duties of individuals requiring separation are identified
	3.1.4.[b]	Responsibility for duties that require separation are assigned to separate individuals
	3.1.4.[c]	Access privileges that enable individuals to exercise the duties that require separations are granted to separate individuals
	Potential assessment methods and objects	
	Examine:	**Select from:** Access control policy, procedures addressing divisions of responsibility and separation of duties, security plan, system configuration settings and associated documentation, list of divisions of responsibility and separation of duties, system access authorizations, system audit records, other relevant documents of records
	Interview:	**Select from: p**ersonnel with responsibilities for defining appropriate divisions of responsibility and separation of duties, personnel with information security responsibilities, system or network administrators
	Test:	**Select from**: mechanisms implementing separation-of-duties policy

Source: *NIST Special Publication 800-171A Assessing Security Requirements for Controlled Unclassified Information*, National Institute of Standards and Technology, June 2018.

NIST Special Publication 800-171 assessments



External assessments



Discussion point

Reporting considerations and communications

Two-way communication

Through the **incident reporting** and **flow-down** requirements, contractors need to establish procedures for communicating to customers and subcontractors.

1

Contractors must evaluate their subcontract requirements for incident reporting and include mechanisms to ensure they are aware of any incident that may impact their data.

2

Determine who within your organization must be informed and at what point external reports should be made.

- Should be determined as part of the incident response plan
- May want to seek legal guidance on what constitutes a “cyber incident” or what qualifies as “evidence of compromise”

3

Subcontractor flow down – monitoring the supply chain

- What are a contractor's responsibilities to protect CDI in their supply chain?
  - Three considerations:
    - Requirements under the DFARS clause
    - Requirements under the Federal Acquisition Regulation
    - Guidance and communications issued by the DoD
- Flow-down DFARS clause in all subcontracts involving CDI or "operationally critical support"
- Prime responsibility for protection of CDI throughout supply chain
- Prime to limit CDI shared with subcontractors

Subcontractor flow down – monitoring the supply chain

Subcontract monitoring industry practices include:

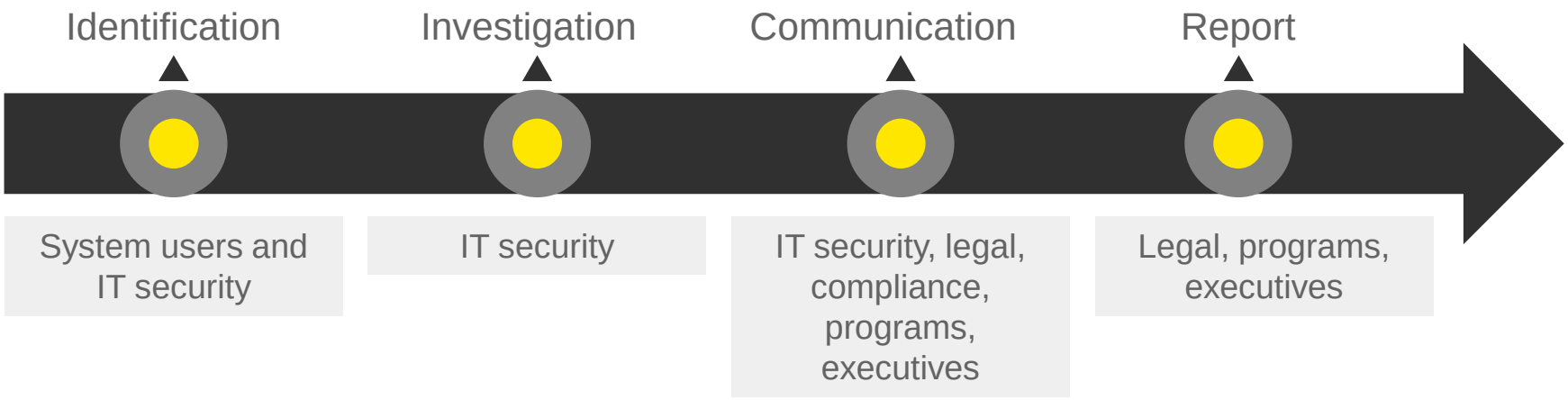
- Develop a risk-based approach based on specified criteria:
  - Program or customer requirements
  - Organizational maturity
  - Data classification
  - Scope of work
- Each subcontract under a contract with clause 252.204-7012 should be evaluated as to the cyber risk associated with providing CDI to complete the scope of work.
- Contractors should incorporate processes for cybersecurity monitoring into their existing subcontractor monitoring processes.
- Utilize appropriate contractual terms and conditions to make certain subcontractors are bound to reporting requirements and are liable for the protection of information.

Incident reporting

- The DFARS clause includes a requirement to report any cyber incident to the DOD within 72 hours.
  - A “cyber incident” is “action[s] taken through the use of computer networks that result[s] in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.”
- The clause requires a contractor to review and notify as follows
  - Review to identify:
    - Compromised computers and servers
    - Specific compromised data
    - Specific compromised user accounts
    - Covered information systems that were part of the cyber incident
    - Other information systems on contractors’ networks that may have been accessed as a result of the incident
- The Defense Industrial Base serves as the portal for all DoD cyber notifications (https://dibnet.dod.mil).

Incident reporting – roles and responsibilities

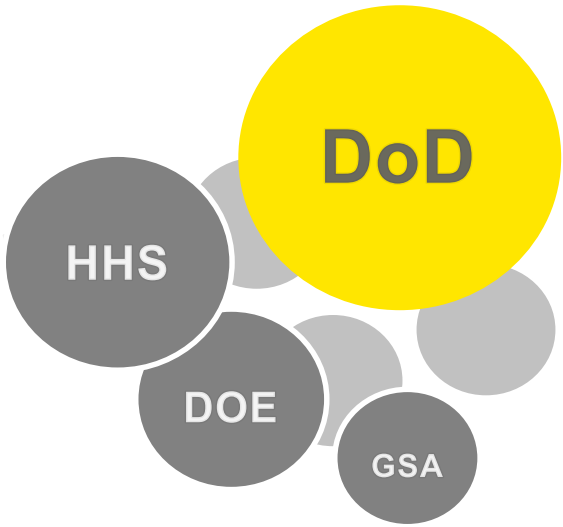
Example of roles within an incident response process



Discussion point

Ongoing considerations

- The DFARS clause is the government's first attempt at controlling information outside of its systems.
- Contractors' contract portfolios and associated scopes of work may look very different than the current state.
- Integrating the NIST control requirements into your IT security framework allows for a flexible and measurable compliance evaluation process.
- Due to the various organizational functions the regulation touches (IT, contracts, legal, compliance, etc.), stakeholders and communication must be established. It cannot be managed effectively within silos.



FAR and General Services Administration proposed rules

	FAR Case 2017-016	GSAR Case 2016-G511	GSAR Case 2016-G515
Purpose	Intended to make certain that the cybersecurity requirements found in the DFARS are applied consistently across all forms of government procurement.	Will require contractors to “protect the confidentiality, integrity and availability of unclassified information and information systems from any risks or threats in accordance with the Federal Information Security Modernization Act of 2014 and associated Federal cybersecurity requirements.”	Will require the reporting of cyber incidents that could potentially affect the GSA or its customer agencies.
Details	Expected to address policies for designating, safeguarding, disseminating, marking, decontrolling, and disposing of controlled CUI.	Will also update existing GSAR clauses 552.239-70, Information Technology Security Plan and Security Authorization, and 552.239-71, Security Requirements for Unclassified Information Technology Resources, to limit use of these clauses to instances when the performance of work requires connection to GSA’s network.	Will require contractors to report “any cyber incident where the confidentiality, integrity, or availability of GSA information or information systems are potentially compromised or where the confidentiality, integrity, or availability of information or information systems owned or managed by or on behalf of the U.S. Government is potentially compromised.” Will also address roles and responsibilities, time frames, contractor requirements, employee training, information preservation and protection requirements, and GSA’s role in the incident reporting process.
Public comments due	March to May 2019	February to April 2019	April to June 2019

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

SCORE no. 05749-191US

1902-3054130

ED None

ey.com