Demystifying Government Cybersecurity

David Kessler, JD

Commercial Cybersecurity Certifications & Standards

- Information Security Management System
- Controls specified in ISO 27002
- Specific controls not mandated (varies)

ISO 27001

- Information security for cloud computing
- Cloud guidance for 37 controls in ISO 27002
- 7 cloud-specific controls

ISO 27017

- Implements ISO 27002 controls applicable to Personally Identifiable Information (PII)
- Used by CSPs who are acting as PII processors

ISO 27018

- Applies to payment card processors
- Storage, processing or transmittal of cardholder or sensitive authentication data

PCI DSS

- Auditing standard for service organizations
- SOC (1-3) reports are internal control reports that assess risk for outsourced services

SSAE 18

- 3-tiered provider assurance program
- Cloud Controls Matrix
- Consensus Assessment Initiative Questionnaire

CSA STAR

- Cybersecurity for financial institutions
- Assessment Tool
  - Inherent Risk Profile
  - Cybersecurity Maturity

FFIEC

- Applies if trading in EU or processing personal data of EU residents
- Breach notifications are mandatory
- Tiered fines (up to 4%)

GDPR

- CIS Controls are a popular set of 20 security controls
- CIS Benchmarks – compare security to consensus standard

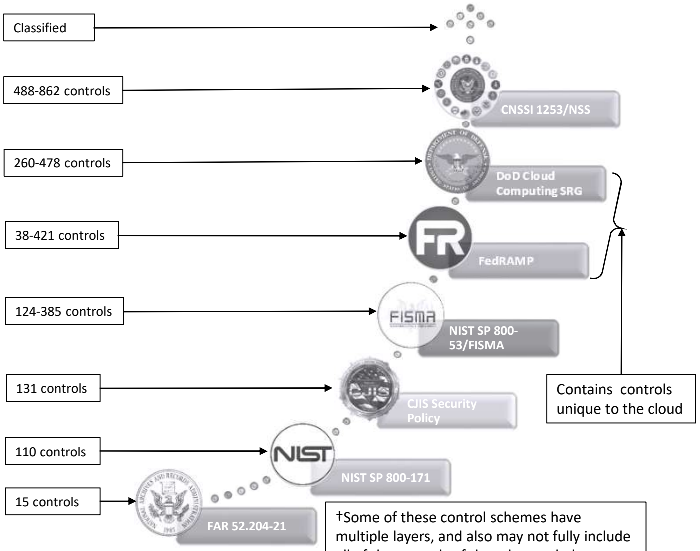
CIS

- Apply to Public Key Infrastructure tech
- Framework for auditors to assess controls of certification authorities

WEBTRUST

Federal Cybersecurity Controls Landscape†

- Federal Government follows escalating scale of controls, depending on system and information requiring protection
- More controls are required at each successively higher level of security and customer type
- Some security control regimes require Assessment and Authorization (A&A) or Authorization to Operate (ATO) by the Federal Government
- State and Local governments follow Federal Government (usually voluntary)
- Some state & local governments have own security controls (e.g., no offshore data storage and/or non-U.S. citizen access to sensitive data)
- NIST Cybersecurity Framework (CSF) also provides guidance for private industry to assess and improve their ability to Identify, Protect, Detect, Respond & Recover (divided into 108 subcategories/controls)



Classified

488-862 controls → CNSSI 1253/NSS

260-478 controls → DoD Cloud Computing SRG

38-421 controls → FedRAMP

124-385 controls → NIST SP 800-53/FISMA

131 controls → CJIS Security Policy

110 controls → NIST SP 800-171

15 controls → FAR 52.204-21

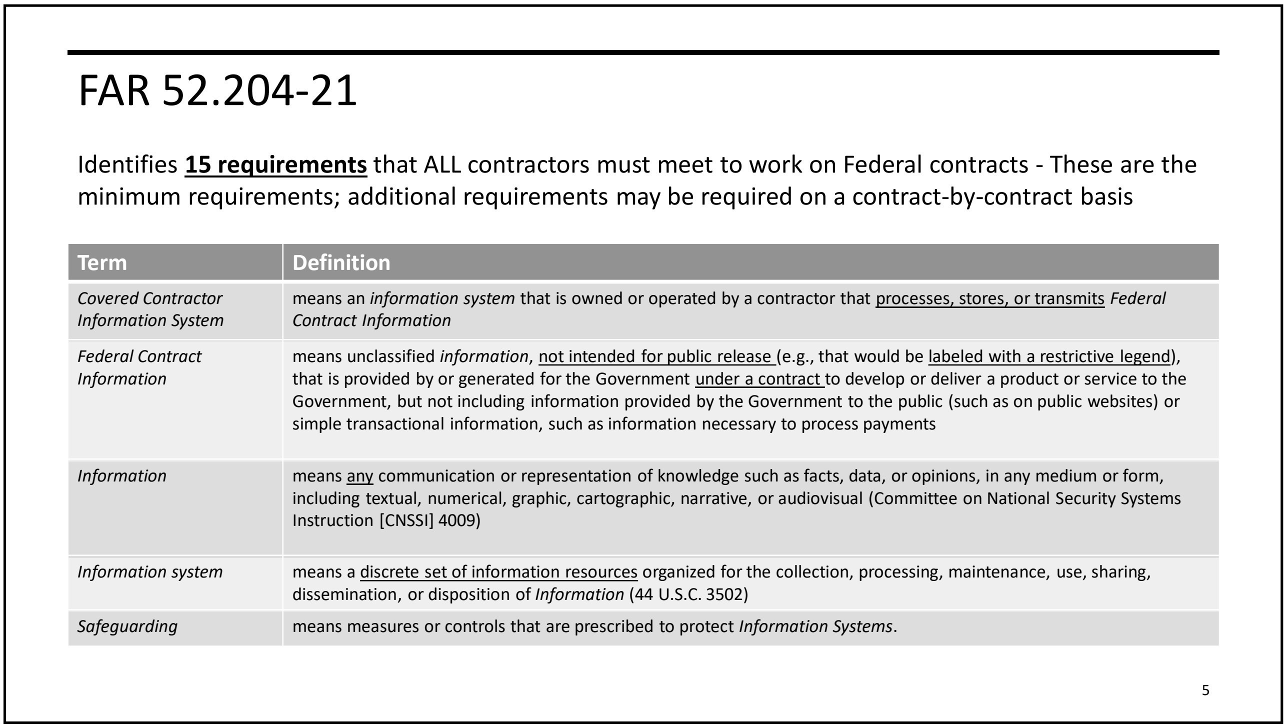
Contains controls unique to the cloud

†"Controls" = controls + enhancements

†Some of these control schemes have multiple layers, and also may not fully include all of the controls of the schemes below them. Plus, agencies may add more controls.

State, Local & Educational Cybersecurity Landscape

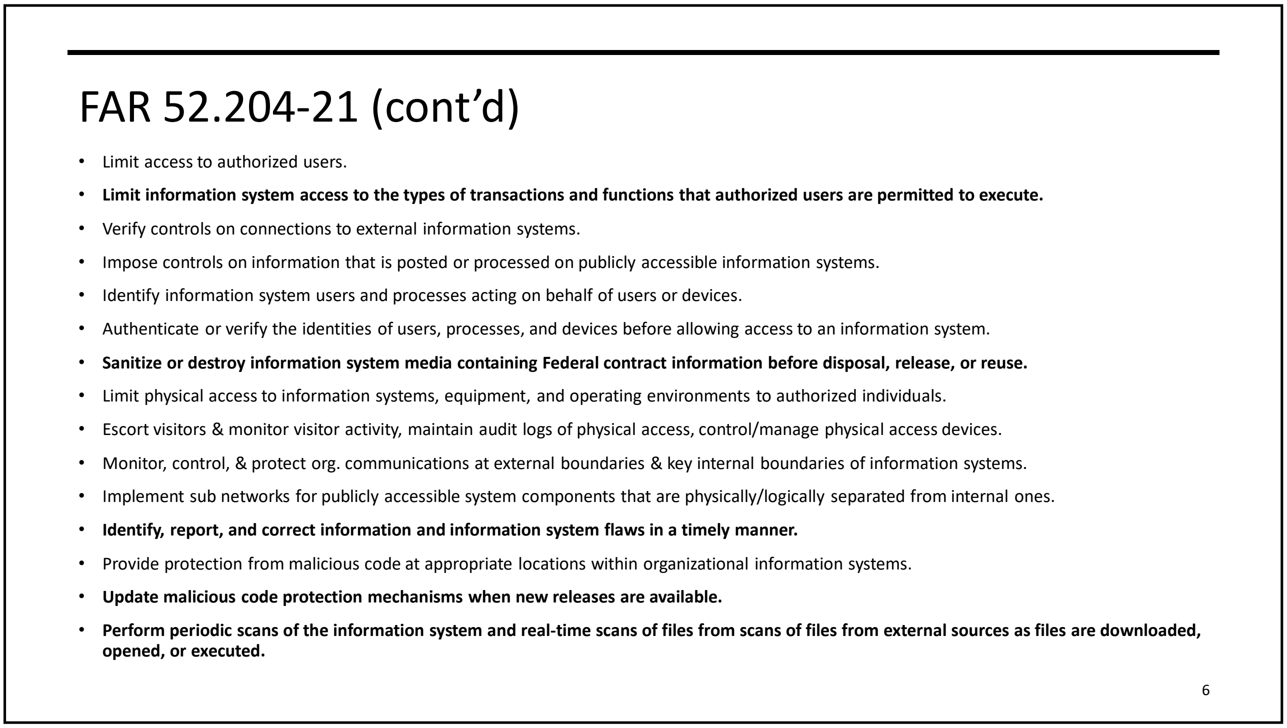
- State & local government and educational (SLED) institutions all have their own unique cybersecurity requirements
- These cybersecurity requirements are intended to protect SLED IT systems, but are flowed down to contractors connecting to IT systems or handling SLED-provided data
- Burgeoning state laws on data privacy and cybersecurity may also be flowed down to contractors having access to, storing or processing consumer data. Examples:
  - California Consumer Privacy Act (CCPA) (AB 375)
  - New York Department of Financial Services Cybersecurity Regulation (23 nycrr 500) Massachusetts Cybersecurity Law
- SLED procurement RFPs often request (or require) that products and services comply with NIST standards, FISMA or FedRAMP (cloud services) and onshore data storage
- SLED cybersecurity landscape is constantly evolving – need to comply with today's cybersecurity standards, but try to "skate to where the puck is going"



FAR 52.204-21

Identifies **<u>15 requirements</u>** that ALL contractors must meet to work on Federal contracts - These are the minimum requirements; additional requirements may be required on a contract-by-contract basis

Term	Definition
Covered Contractor Information System	means an *information system* that is owned or operated by a contractor that <u>processes, stores, or transmits</u> *Federal Contract Information*
Federal Contract Information	means unclassified *information*, <u>not intended for public release</u> (e.g., that would be <u>labeled with a restrictive legend</u>), that is provided by or generated for the Government <u>under a contract</u> to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as information necessary to process payments
Information	means <u>any</u> communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual (Committee on National Security Systems Instruction [CNSSI] 4009)
Information system	means a <u>discrete set of information resources</u> organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of *Information* (44 U.S.C. 3502)
Safeguarding	means measures or controls that are prescribed to protect *Information Systems*.

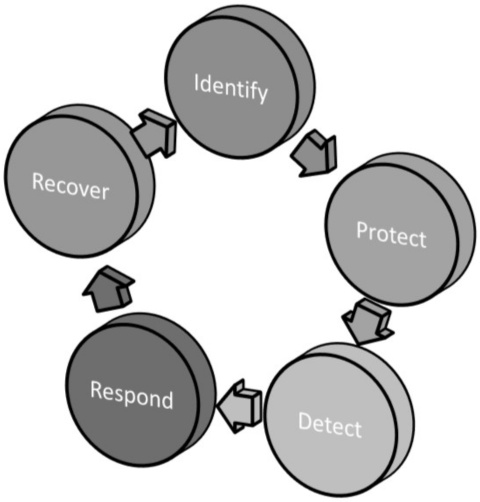


FAR 52.204-21 (cont'd)

- Limit access to authorized users.
- **Limit information system access to the types of transactions and functions that authorized users are permitted to execute.**
- Verify controls on connections to external information systems.
- Impose controls on information that is posted or processed on publicly accessible information systems.
- Identify information system users and processes acting on behalf of users or devices.
- Authenticate or verify the identities of users, processes, and devices before allowing access to an information system.
- **Sanitize or destroy information system media containing Federal contract information before disposal, release, or reuse.**
- Limit physical access to information systems, equipment, and operating environments to authorized individuals.
- Escort visitors & monitor visitor activity, maintain audit logs of physical access, control/manage physical access devices.
- Monitor, control, & protect org. communications at external boundaries & key internal boundaries of information systems.
- Implement sub networks for publicly accessible system components that are physically/logically separated from internal ones.
- **Identify, report, and correct information and information system flaws in a timely manner.**
- Provide protection from malicious code at appropriate locations within organizational information systems.
- **Update malicious code protection mechanisms when new releases are available.**
- **Perform periodic scans of the information system and real-time scans of files from scans of files from external sources as files are downloaded, opened, or executed.**

NIST Cybersecurity Framework

- NIST Framework for Improving Critical Infrastructure Cybersecurity (CSF) is a set of **"optional"** standards, best practices, and recommendations for improving cybersecurity at the organizational level—
  - No mandatory security controls.
  - Mandatory for federal agencies.
  - Heavily adopted commercially.
- CSF features 5 functions used to organize cybersecurity to form a top-level approach to securing systems and responding to threats.
- CSF has 4 tiers of implementation; but not considered "maturity levels."



7

NIST SP 800-171

- NIST Special Publication 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations"
- Defines how to safeguard and distribute controlled unclassified information (CUI) on government contractor information systems
- Contains 14 categories of security controls divided into *Basic Security Requirements* & *Derived Security Requirements*
- Incorporated into DoD contracts and required for all suppliers, including those supplying commercial items (but not commercial-off-the-shelf items) (DFARS 252.204-7012)
- Contractors may limit the scope of the CUI security requirements to particular systems or network components

8

NIST SP 800-171 cont’d

Security Control Families

- Access Control
- Awareness & Training
- Audit & Accountability
- Configuration Management
- Identification & Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical Protection
- Personnel Security
- Risk Assessment
- Security Assessment
- System & Communications Protection
- System & Information Integrity

New Developments [Proposed NIST SP 800-171B]

- In June 2019, NIST released SP 800-171B, which includes 33 enhanced CUI requirements for “critical systems” and “high value assets”
- The focus of these new requirements is on organizations that are likely targets of advanced persistent threat (APT) attacks.
- “Critical systems” and high value assets” are not defined in 800-171B
- No criteria questions to help determine what qualifies as a critical system or high value asset
- Unclear how a contractor will be notified by an agency that it is operating a critical program or high value asset
- Unclear whether an agency can designate a critical system or high value asset after contract award and during contract performance

National Archives & Records Administration [Civilian]

- Executive Order 13556 authorized the National Archives and Records Administration (NARA) to create a program for managing controlled unclassified information (CUI) across the executive branch
- The NARA CUI Registry is an online repository for information, guidance, policy, and requirements on handling CUI (identifies/defines categories and subcategories of CUI)
- Procedures for use of CUI, such as marking, safeguarding, transporting, disseminating, reusing, and disposing of CUI
- New *FAR* clause pending from NARA regarding CUI; expected to incorporate NIST SP 800-171
- In the interim, most federal contracts contain FAR 52.204-21, "Basic Safeguarding of Covered Contractor Information Systems," requiring 15 basic security controls as part of a contractor's routine business practices

DFARS 252.204-7012 [Compliance]

- Applies to all DoD contracts and subcontracts (except if solicitation is solely for *commercial-off-the-shelf* products/services) and requires enhanced safeguarding of *covered contractor information systems* that contain *Covered Defense Information* (CDI)
- Mandatory flow-down clause in subcontracts at all tiers for *operationally critical support* **or** where subcontract performance will involve *covered contractor information system with CDI*
- Must provide *adequate security* for covered systems with CDI; at minimum must have been compliant with NIST 800-171 not later than December 31, 2017
- Can submit "alternative yet equally effective" controls to DoD CIO for approval.
- Must rapidly report *cyber incidents* on *covered contractor information systems* with *CDI*, or that affect the contractor's ability to perform *operationally critical support* under a contract, and comply with other obligations essential to documenting the cyber incident.
- DoD will not currently certify that a contractor is compliant with NIST SP 800-171, and third-party assessments or certifications of compliance not required, authorized, nor recognized by DoD (**this is changing** – See proposed "Cybersecurity Maturity Model Certification" (CMMC) requiring 3rd party or government auditing)

DFARS 252.204-7012 [Cyber Incident Reporting]

- Contractors must report *cyber incidents* on covered contractor information systems with CDI, or that affect the contractor's ability to perform operationally critical support under a contract
  - Upon discovery, must conduct a review for evidence of compromise
  - Rapidly report within **72 hours** directly to DOD via specified online portal (https://dibnet.dod.mil).
  - Must provide DOD-assigned incident report number to prime/higher-tiered subcontractor(s)
  - Must preserve and protect images of known affected images and systems for 90 days
  - Must provide DOD access to additional information or equipment necessary to conduct forensics analysis
  - Must submit any malicious software uncovered to DOD Cyber Crime Center (DC3), not the contracting officer
- A *cyber incident* that is reported by a contractor shall not, by itself, be interpreted as evidence that the contractor has failed to provide *adequate security* on its *covered contractor information systems*, or has otherwise failed to meet the regulation

DFARS 252.204-7012 [Use of Cloud Services]

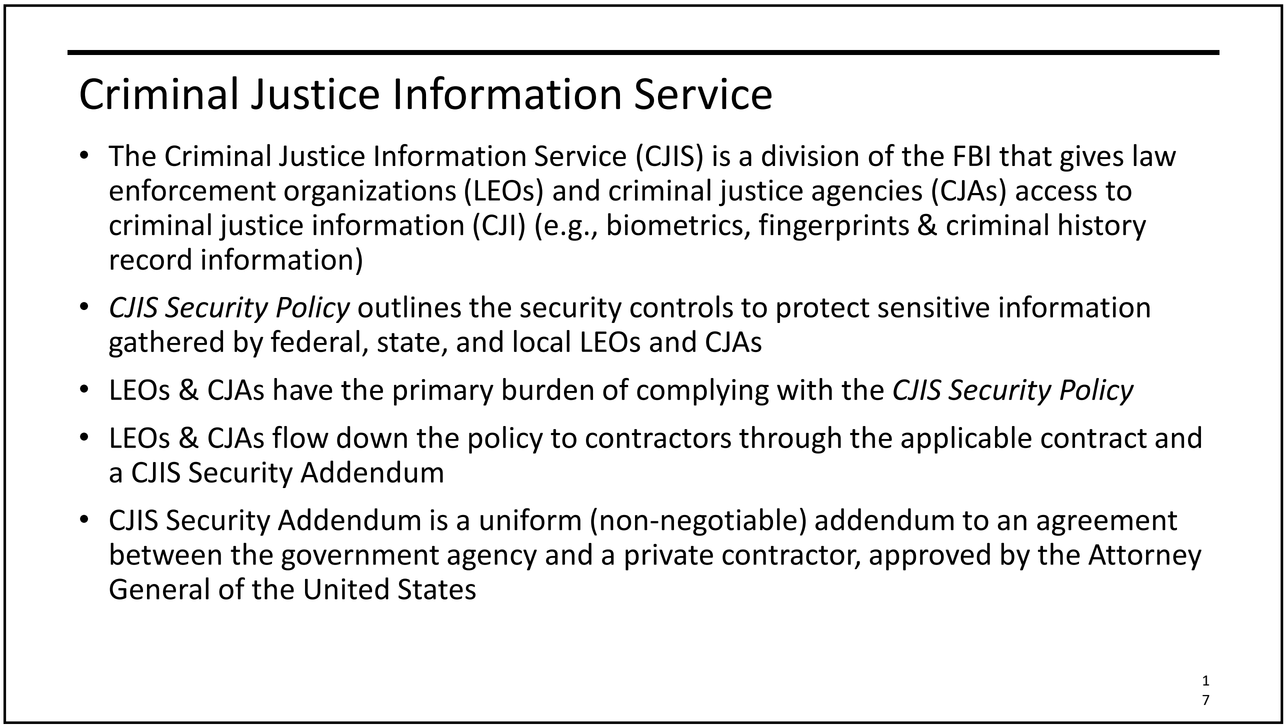
- If the contractor intends to use an external cloud service provider (CSP) to store, process, or transmit any CDI in performance of the contract, it must require and ensure that it meets security requirements equivalent to those in FedRAMP Moderate baseline
- If after the award of a DoD contract, the contractor proposes to use cloud computing services in the performance of the contract, it must obtain approval from the DoD Contracting Officer prior to utilizing such cloud services
- CSP must comply with requirements for cyber-incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber-incident damage assessment
- Contractor must maintain within the U.S. or outlying areas all Government data that is not physically located on DoD premises, unless the Contractor receives written notification from the Contracting Officer to use another location

DFARS 252.204-7012 [Subcontracting]

- The Undersecretary of Defense issued a memo on January 21, 2019, addressing cybersecurity oversight as part of a contractor’s purchasing system review
- DCMA will leverage its review of a contractor's purchasing system in accordance with DFARS 252.244-7001, “Contractor Purchasing System Administration,” to:
  - Review contractor procedures to ensure contractual DOD requirements for marking and distribution statements on DOD CUI flow down appropriately to its Tier 1 level suppliers.
  - Review contractor procedures to assess compliance of its Tier 1 level suppliers with DFARS 252.204-7012 and NIST SP 800-171
- To ensure that a similar approach may be taken at companies for which DCMA does not administer contracts (such as the Secretary of the Navy's shipbuilding contracts), DOD will work with representatives of those communities to implement a similar solution

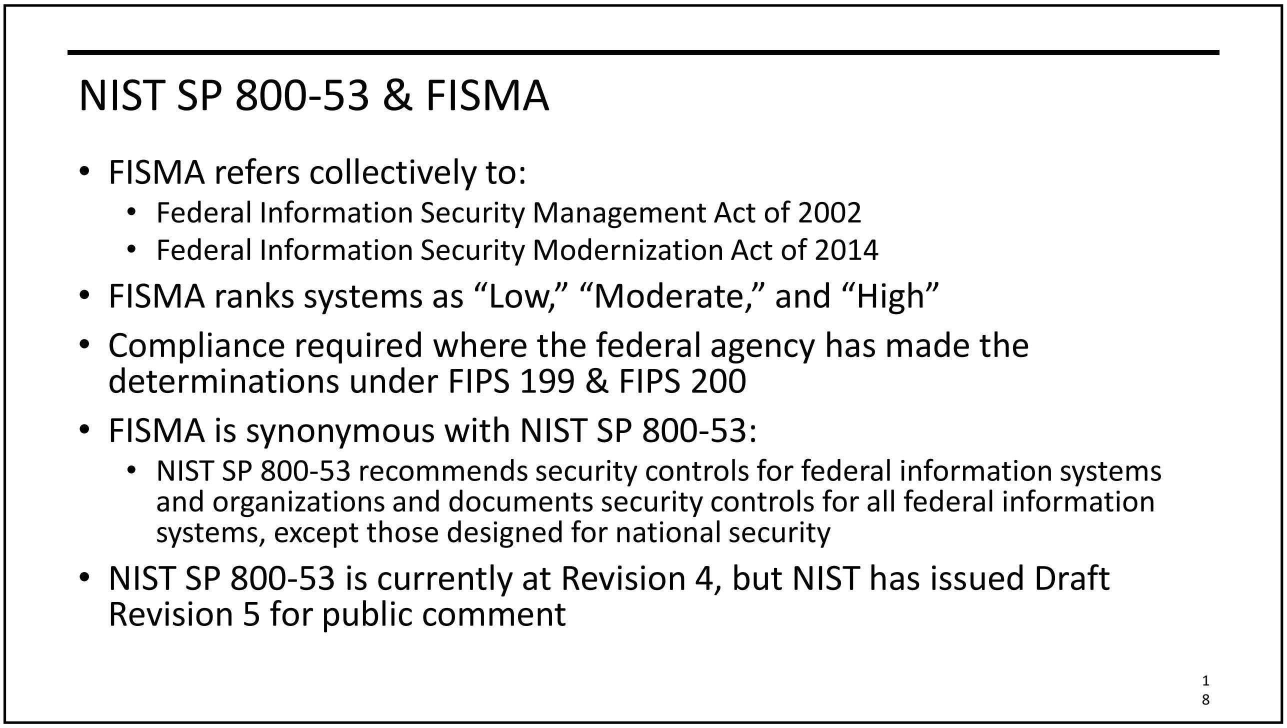
New DoD Developments [Proposed CMMC]

- Companies doing business with DoD, including subcontractors, may need to obtain a Cybersecurity Maturity Model Certification (CMMC) from the DoD
- CMMC is expected to combine relevant portions of various cybersecurity standards, such as NIST SP 800-171, NIST SP 800-53, ISO 270001, and ISO 27032, into one unified standard for cybersecurity
- Unlike NIST SP 800-171, which measures a contractor’s compliance with a specified set of controls, CMMC will more broadly “measure the maturity of a company’s institutionalization of cybersecurity practices and processes.”
- CMMC expected to designate maturity levels – range is “Basic Cybersecurity Hygiene” to “Advanced”
- DoD will assess which CMMC level is appropriate for a particular contract as a “go/no go” evaluative determination (similar to UK’s MOD)
- Contractors will be required to be certified by a third-party auditor, but “higher level assessments” may be conducted by government assessors
- Compromise of a contractor’s systems will not result in automatic loss of certification (but may require recertification)
- Cost of certification will be considered an allowable, reimbursable cost



Criminal Justice Information Service

- The Criminal Justice Information Service (CJIS) is a division of the FBI that gives law enforcement organizations (LEOs) and criminal justice agencies (CJAs) access to criminal justice information (CJI) (e.g., biometrics, fingerprints & criminal history record information)
- *CJIS Security Policy* outlines the security controls to protect sensitive information gathered by federal, state, and local LEOs and CJAs
- LEOs & CJAs have the primary burden of complying with the *CJIS Security Policy*
- LEOs & CJAs flow down the policy to contractors through the applicable contract and a CJIS Security Addendum
- CJIS Security Addendum is a uniform (non-negotiable) addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States



NIST SP 800-53 & FISMA

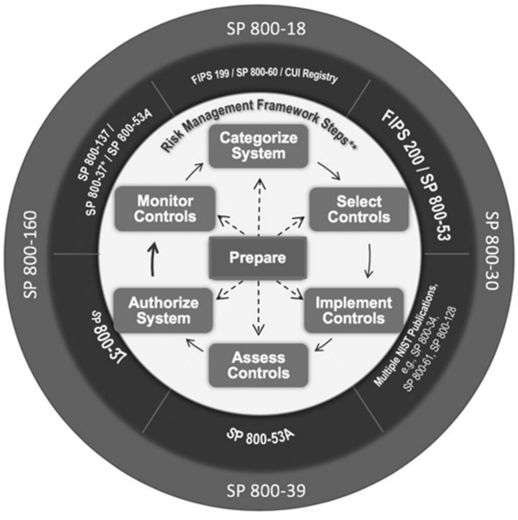
- FISMA refers collectively to:
  - Federal Information Security Management Act of 2002
  - Federal Information Security Modernization Act of 2014
- FISMA ranks systems as “Low,” “Moderate,” and “High”
- Compliance required where the federal agency has made the determinations under FIPS 199 & FIPS 200
- FISMA is synonymous with NIST SP 800-53:
  - NIST SP 800-53 recommends security controls for federal information systems and organizations and documents security controls for all federal information systems, except those designed for national security
- NIST SP 800-53 is currently at Revision 4, but NIST has issued Draft Revision 5 for public comment

Federal Information Processing Standards

- The Federal Information Processing Standards (FIPS) are a set of standards published by the National Institute of Standards and Technology (NIST)
- FIPS describe document processing, encryption algorithms, and other IT standards for use within civilian government agencies and by contractors to comply with FISMA
- FIPS 140-2: Specifies the security requirements for cryptographic modules protecting sensitive information
- FIPS 199: Categorizes the risk of a system according to “confidentiality,” “integrity,” and “availability”; then divides the systems into ”high,” “moderate,” and “low” impact systems based on their impact on individuals and organizations
- FIPS 200: Specifies the minimum security requirements (in 17 areas) for civilian federal information systems

NIST SP 800-37 (Risk Management Framework)

- The Risk Management Framework (RMF) is a set of criteria that dictate how U.S. government IT systems must be architected, secured, and monitored.
  - Originally developed by DOD, the RMF was adopted by the rest of the federal government in 2010
- RMF is a process to architect and engineer a data security process for new IT systems:
  - Step 1: Categorize Information System
  - Step 2: Select Security Controls
  - Step 3: Implement Security Controls
  - Step 4: Assess Security Controls
  - Step 5: Authorize Information System
  - Step 6: Monitor Security Controls
- In addition to the primary document (SP 800-37), the RMF uses supplemental documents SP 800-30, SP 800-39, SP 800-53, SP 800-53A, and SP 800-137

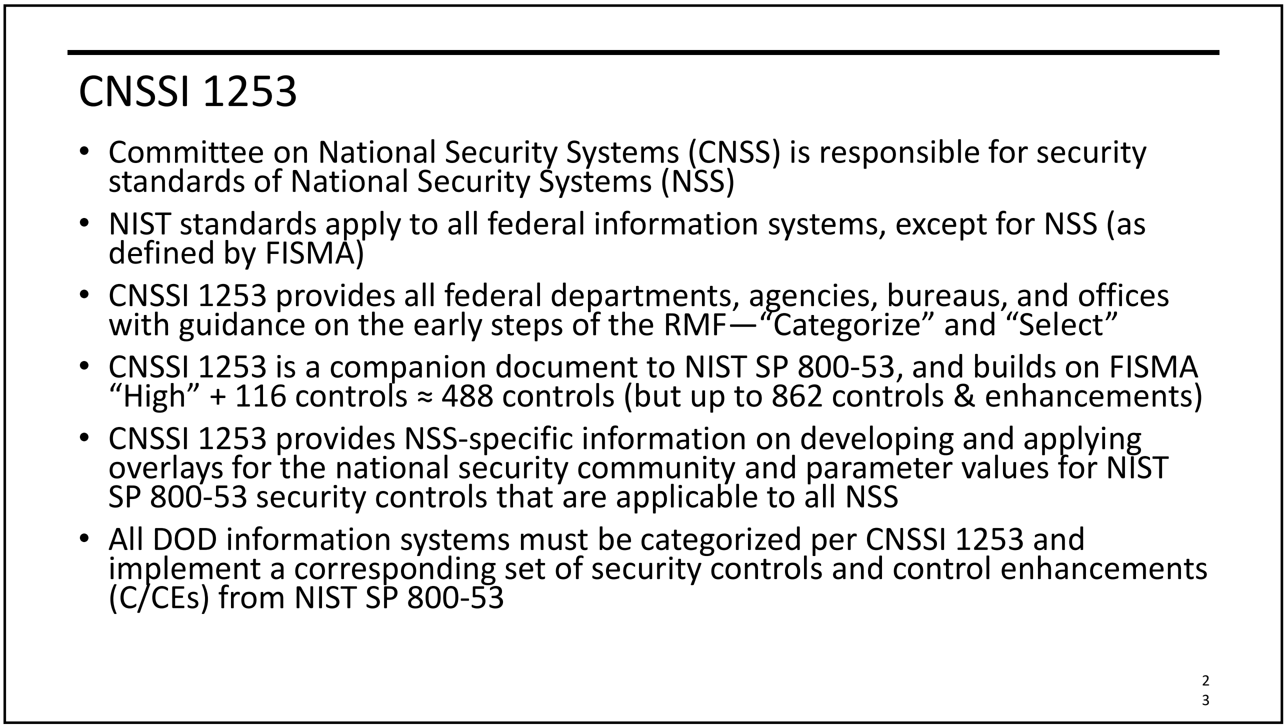


FedRAMP

- Federal Risk and Authorization Management Program (FedRAMP) provides a standardized approach to security assessment, authorization, and continuous monitoring (ConMon) for cloud service offerings (CSOs)
- FedRAMP uses the NIST Federal Information Processing Standards (FIPS) and FISMA 800-53 defined control standards
- FedRAMP ranks CSOs at “LI SaaS” (38 controls), “Low” (125 controls), “Moderate” (325 controls), and “High” (421 controls)
- There are two ways to authorize a CSO under FedRAMP:
  - Joint Authorization Board (JAB) provisional authorization to operate (P-ATO), and
  - Through individual agencies
- Consultants help get CSOs “FedRAMP Ready,” while Third Party Assessment Organizations (3PAO) perform the security assessments of CSOs
- The federal agency consuming the service still has final responsibility for final authority to operate

DoD Cloud Computing Security Requirements

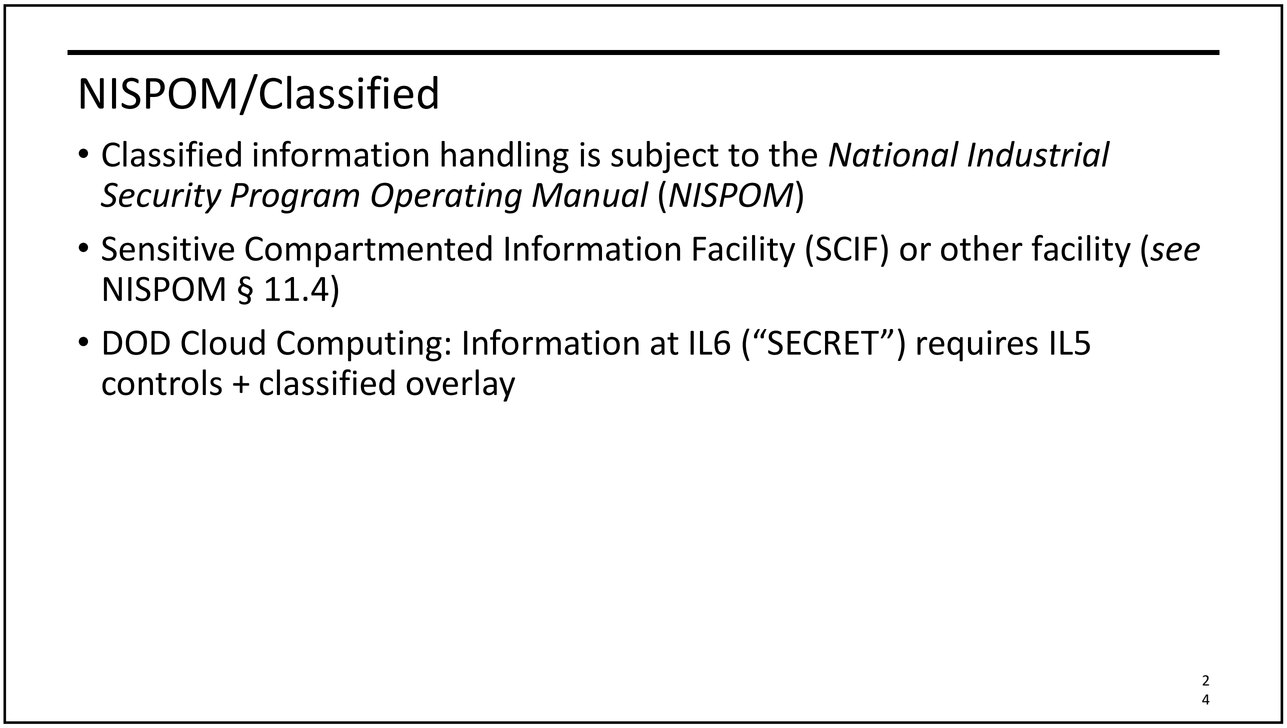
- The Defense Information Systems Agency (DISA) developed the *DOD Cloud Computing Security Requirements Guide* (*SRG*)
  - Defines the baseline security requirements for cloud service providers (CSPs) that host DOD information, systems, and applications, and for DOD’s use of cloud services
  - Maps to the DOD Risk Management Framework, NIST SP 800-37, and NIST SP 800-53, and can leverage FedRAMP.
  - Leverages FedRAMP “Moderate” (325 controls + additional controls for IL4, IL5, and IL6 – up to ~478 controls)
  - Provides standard assessment and authorization process for CSPs to obtain a DOD Provisional Authorization (PA), which allows DOD components to leverage the CSP’s environment without individualized assessment and authorization.
  - Rates risk by Impact Level (IL) (e.g., IL4, IL5)



CNSSI 1253

- Committee on National Security Systems (CNSS) is responsible for security standards of National Security Systems (NSS)
- NIST standards apply to all federal information systems, except for NSS (as defined by FISMA)
- CNSSI 1253 provides all federal departments, agencies, bureaus, and offices with guidance on the early steps of the RMF—“Categorize” and “Select”
- CNSSI 1253 is a companion document to NIST SP 800-53, and builds on FISMA “High” + 116 controls ≈ 488 controls (but up to 862 controls & enhancements)
- CNSSI 1253 provides NSS-specific information on developing and applying overlays for the national security community and parameter values for NIST SP 800-53 security controls that are applicable to all NSS
- All DOD information systems must be categorized per CNSSI 1253 and implement a corresponding set of security controls and control enhancements (C/CEs) from NIST SP 800-53

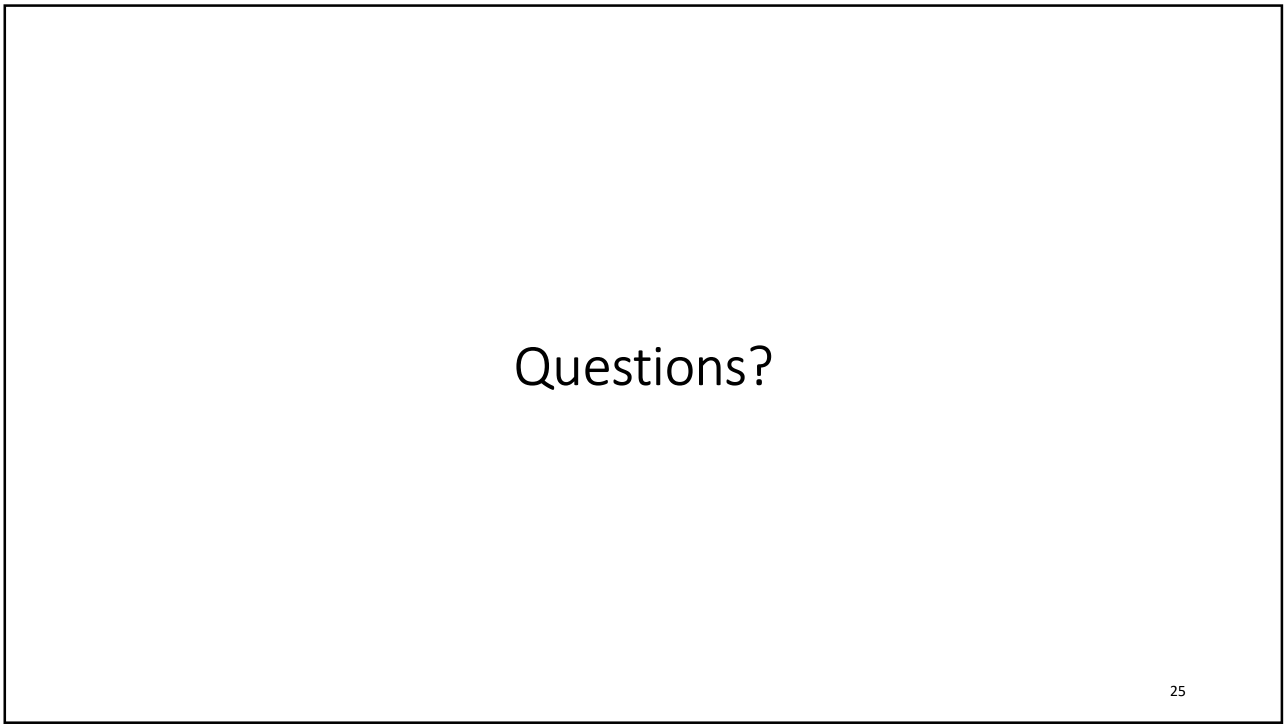
23



NISPOM/Classified

- Classified information handling is subject to the *National Industrial Security Program Operating Manual* (*NISPOM*)
- Sensitive Compartmented Information Facility (SCIF) or other facility (*see* NISPOM § 11.4)
- DOD Cloud Computing: Information at IL6 (“SECRET”) requires IL5 controls + classified overlay

24



Questions?

25