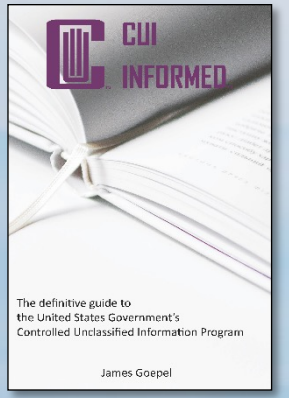
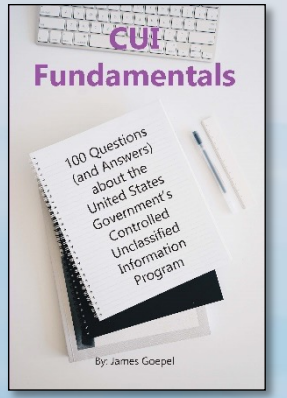
DIB Cybersecurity

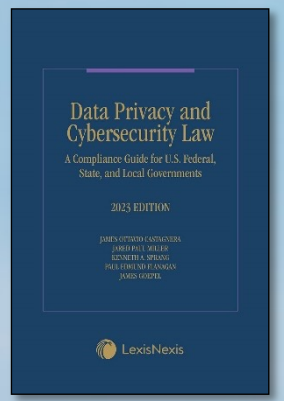
The How and Why
Behind the CMMC Program

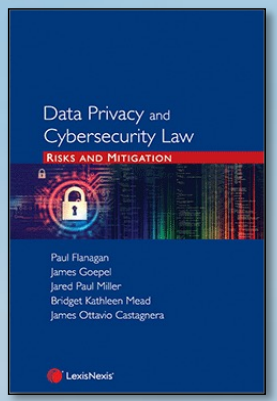
About Me

- General Counsel and Director of Education at FutureFeed (https://FutureFeed.co)
- Founding Director of the CMMC Accreditation Body (Cyber AB) (Prev.)
  - Provisional CMMC Instructor (PI), Certified CMMC Assessor (CCA), Certified CMMC Professional (CCP)
  - Created and taught the original RP training program
  - Board Treasurer
- Co-Founder of the CMMC Information Institute
- Author
  - 2 books on Controlled Unclassified Information (https://CUIInformed.com)
  - Certified CMMC Professional (CCP) curriculum (Co-author)
  - 2 books on cybersecurity law (Co-author)
- Adjunct Faculty at RIT; former Adjunct Professor at Drexel University
- Expert Witness in Government Contract Cybersecurity Cases
- JD and LLM – George Mason University
  - Advisor to many government contractors including Unisys and JHU/APL
- BSECE – Drexel University
  - Designed satellite test equipment and processes
  - Systems Administrator and Developer for the US Congress (House of Representatives)



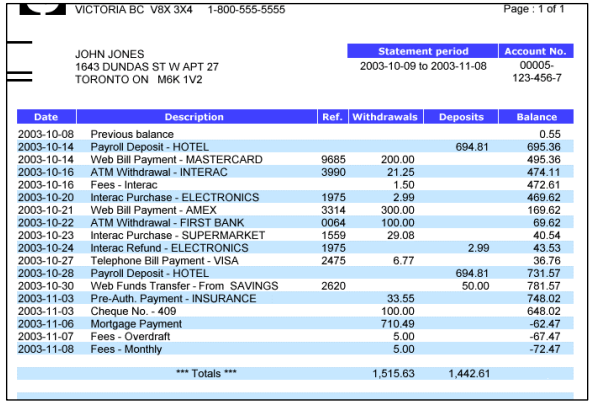






Background

- Your organization generates a lot of sensitive information, such as:
  - New product designs
  - Business plans
  - Banking and other financial information
  - Human resources records
- Your organization also receives and handles other sensitive information, such as:
  - Employee social security numbers
  - Employee banking information (Direct Deposit)
  - Partner/vendor information and product designs
  - Client information

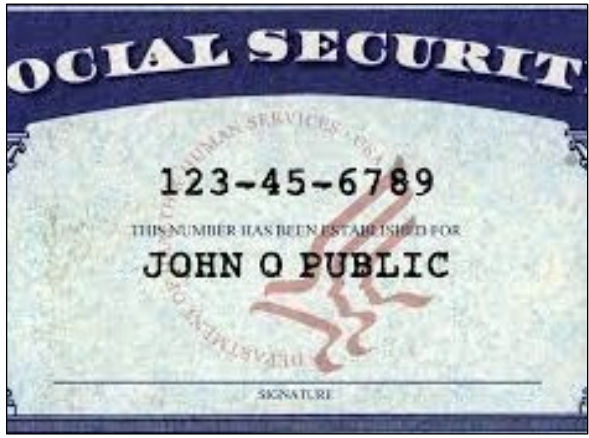


VICTORIA BC V8X 3X4 1-800-555-5555 Page : 1 of 1

JOHN JONES
1643 DUNDAS ST W APT 27
TORONTO ON M6K 1V2

Statement period	Account No.
2003-10-09 to 2003-11-08	00005-123-456-7

Date	Description	Ref.	Withdrawals	Deposits	Balance
2003-10-08	Previous balance				0.55
2003-10-14	Payroll Deposit - HOTEL			694.81	695.36
2003-10-14	Web Bill Payment - MASTERCARD	9685	200.00		495.36
2003-10-16	ATM Withdrawal - INTERAC	3990	21.25		474.11
2003-10-16	Fees - Interac		1.50		472.61
2003-10-20	Interac Purchase - ELECTRONICS	1975	2.99		469.62
2003-10-21	Web Bill Payment - AMEX	3314	300.00		169.62
2003-10-22	ATM Withdrawal - FIRST BANK	0064	100.00		69.62
2003-10-23	Interac Purchase - SUPERMARKET	1559	29.08		40.54
2003-10-24	Interac Refund - ELECTRONICS	1975		2.99	43.53
2003-10-27	Telephone Bill Payment - VISA	2475	6.77		36.76
2003-10-28	Payroll Deposit - HOTEL			694.81	731.57
2003-10-30	Web Funds Transfer - From SAVINGS	2620		50.00	781.57
2003-11-03	Pre-Auth. Payment - INSURANCE		33.55		748.02
2003-11-03	Cheque No. - 409		100.00		648.02
2003-11-06	Mortgage Payment		710.49		-62.47
2003-11-07	Fees - Overdraft		5.00		-67.47
2003-11-08	Fees - Monthly		5.00		-72.47
	*** Totals ***		1,515.63	1,442.61	



What Makes Information Sensitive?

- Unauthorized disclosure can lead to adverse consequences, such as:
  - Increased competition
  - Lost/stolen revenue
  - Identity theft
  - Cyber stalking
  - Personal/family issues

- At a minimum, dealing with the loss of sensitive information is distracting for the entity whose information is disclosed.
- But it can also lead to much larger issues.

Organizations and Sensitive Information

- When the adverse consequences are likely to directly impact their business, organizations are often more careful with sensitive information.
- When the potential adverse consequences only impact a third party, including clients, employees, etc., organizations often are not as careful with the sensitive information.
- How do companies get their business partners or vendors to pay more attention to safeguarding sensitive information?
  - Make it a contractual requirement

Contract Requirements

- Contracts typically require:
  - Same level of safeguarding as your own sensitive information
  - Not less than reasonable care
- What is “reasonable care”?
- It must have a solid, defensible foundation.
- It can’t be a house of cards.

We will circle back to this a little later.

Laws and Regulations

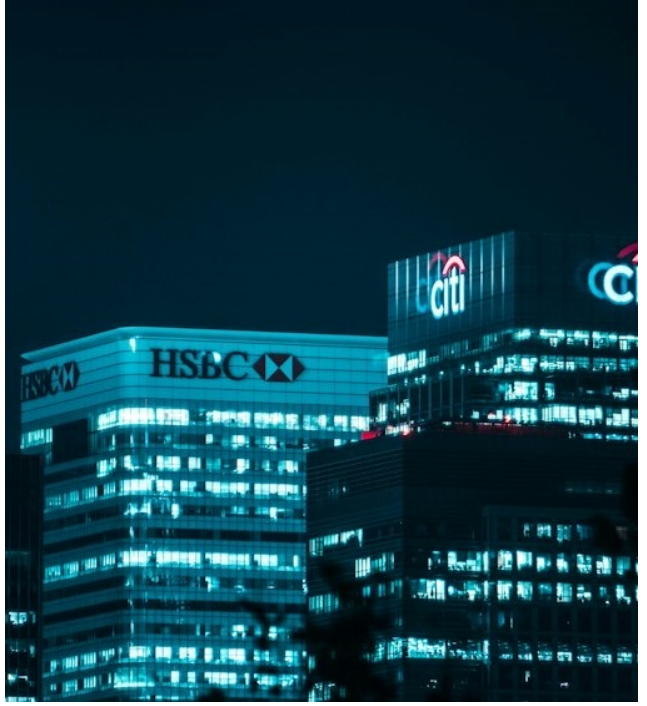
- Most consumers and employees do not have the same bargaining power as organizations.
- They typically can't get their vendors to agree to accept safeguarding requirements as contractual requirements.
- Legislators and regulators are (eventually) spurred into action by consumer and employee complaints when consumers' and employees' information is not properly protected.

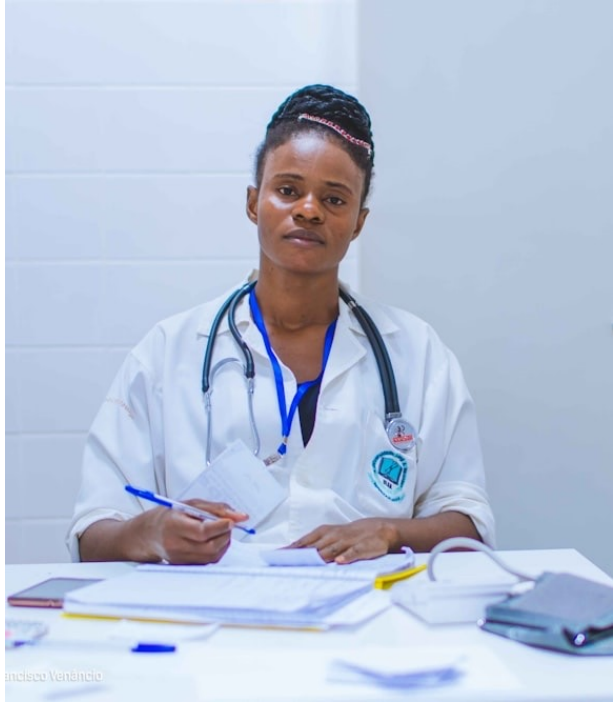
Legal and Regulatory Compliance

- Legislation and regulations seek to shift the cost of protecting information onto the recipient.
- The laws and regulations impose significant fines and penalties, and may even subject organizational leadership and employees to jail time, for failing to comply with the requirements.
- This forces the recipient to pay more attention to securing the information.

Examples

- Health Insurance Portability and Accountability Act (“HIPAA”)
- Personally Identifiable Information (e.g., California Consumer Privacy Act (“CCPA”), Graham Leach Bliley Act (“GLBA”), etc.)
- Banking Information (NY DFS Rule 500)
- Many of these laws and regulations require “reasonable” cybersecurity programs to protect privacy data.





Federal Government Information

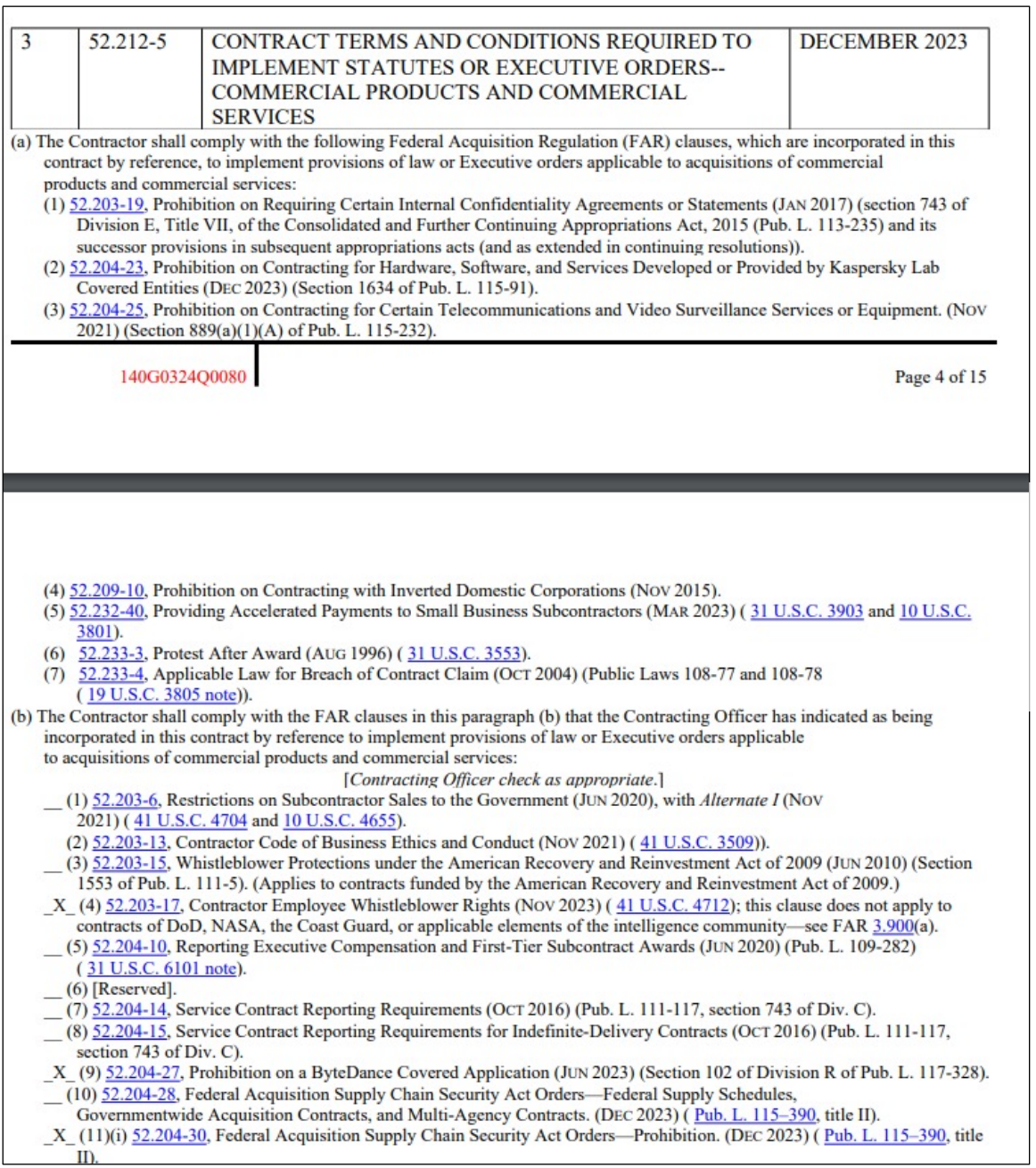
- Like your business, the federal government creates and receives a lot of sensitive information, including:
  - Employee social security numbers
  - Human resources information
  - Healthcare information
  - Income tax information
  - Proposals from contractors
  - Research and development
- That information is typically subject to the same federal laws and regulations as your organization faces. And sometimes Congress adds more.
- Agencies can also proactively pass regulations that require safeguarding of sensitive information.

Government Contractors

- The government relies heavily on federal contractors.
  - $694B in contract spending in 2022
- Contractors are often asked to either:
  - Process information on behalf of the government; or
  - Create information for the government.
- The agency that hired the contractor can be liable for any breaches or other incidents, including “spills,” of sensitive information.

Government's Response

- Just like their commercial colleagues:
  - Add safeguarding requirements to contracts
- All Executive Branch agencies: Federal Acquisition Regulations ("FAR")
  - Establishes minimum baselines and consistent approaches to doing business with the government.
- Agency-specific contract "supplements" (e.g., Defense Federal Acquisition Regulations "DFARS")
  - Clarifies and enhances the baselines established in the FAR.
  - Includes agency-specific requirements.



3	52.212-5	CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS--COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES	DECEMBER 2023

(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses, which are incorporated in this contract by reference, to implement provisions of law or Executive orders applicable to acquisitions of commercial products and commercial services:
(1) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (JAN 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).
(2) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab Covered Entities (DEC 2023) (Section 1634 of Pub. L. 115-91).
(3) 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (NOV 2021) (Section 889(a)(1)(A) of Pub. L. 115-232).

140G0324Q0080 Page 4 of 15

(4) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (NOV 2015).
(5) 52.232-40, Providing Accelerated Payments to Small Business Subcontractors (MAR 2023) (31 U.S.C. 3903 and 10 U.S.C. 3801).
(6) 52.233-3, Protest After Award (AUG 1996) (31 U.S.C. 3553).
(7) 52.233-4, Applicable Law for Breach of Contract Claim (OCT 2004) (Public Laws 108-77 and 108-78 (19 U.S.C. 3805 note)).

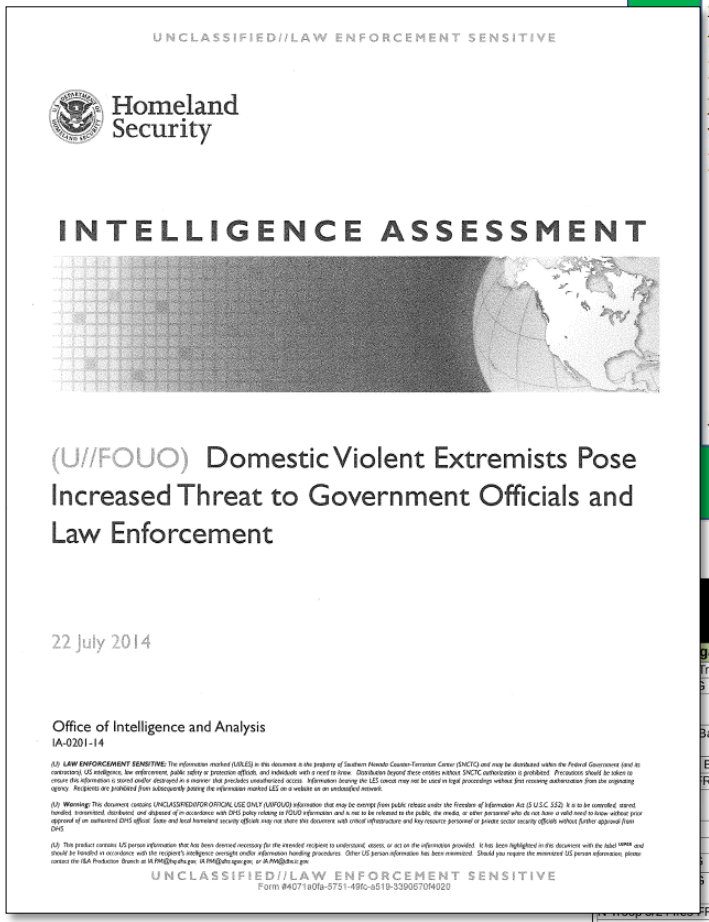
(b) The Contractor shall comply with the FAR clauses in this paragraph (b) that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial products and commercial services:
[*Contracting Officer check as appropriate.*]
__ (1) 52.203-6, Restrictions on Subcontractor Sales to the Government (JUN 2020), with *Alternate I* (NOV 2021) (41 U.S.C. 4704 and 10 U.S.C. 4655).
(2) 52.203-13, Contractor Code of Business Ethics and Conduct (NOV 2021) (41 U.S.C. 3509)).
__ (3) 52.203-15, Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (JUN 2010) (Section 1553 of Pub. L. 111-5). (Applies to contracts funded by the American Recovery and Reinvestment Act of 2009.)
_X_ (4) 52.203-17, Contractor Employee Whistleblower Rights (NOV 2023) (41 U.S.C. 4712); this clause does not apply to contracts of DoD, NASA, the Coast Guard, or applicable elements of the intelligence community—see FAR 3.900(a).
__ (5) 52.204-10, Reporting Executive Compensation and First-Tier Subcontract Awards (JUN 2020) (Pub. L. 109-282) (31 U.S.C. 6101 note).
__ (6) [Reserved].
__ (7) 52.204-14, Service Contract Reporting Requirements (OCT 2016) (Pub. L. 111-117, section 743 of Div. C).
__ (8) 52.204-15, Service Contract Reporting Requirements for Indefinite-Delivery Contracts (OCT 2016) (Pub. L. 111-117, section 743 of Div. C).
_X_ (9) 52.204-27, Prohibition on a ByteDance Covered Application (JUN 2023) (Section 102 of Division R of Pub. L. 117-328).
__ (10) 52.204-28, Federal Acquisition Supply Chain Security Act Orders—Federal Supply Schedules, Governmentwide Acquisition Contracts, and Multi-Agency Contracts. (DEC 2023) (Pub. L. 115–390, title II).
_X_ (11)(i) 52.204-30, Federal Acquisition Supply Chain Security Act Orders—Prohibition. (DEC 2023) (Pub. L. 115–390, title II).

Government Contracts

- Dozens (or more) of clauses incorporated by reference or explicitly included in the contract.
- Contractors are expected to have read and understood all applicable clauses.
- When contractors sign a contract, they are attesting to the fact that they meet (i.e., comply with) the requirements described in all applicable clauses.
- Failure to meet the material, applicable requirements can result in termination or non-renewal of contracts and even False Claims Act penalties.
- Two common problems for contractors:
  - Addition of new, “mandatory” clauses
  - Editing of existing clauses

Back in the Day

- The government has sought to identify and protect sensitive information for decades.
- Over 100 different "sensitive information" designations were created, including:
  - For Official Use Only ("FOUO")
  - Sensitive but Unclassified ("SBU")
  - Law Enforcement Sensitive ("LES")
- Each agency had its own approach to identifying the information.
- Each agency defined its own safeguarding requirements and incorporated them into its contract supplements.


UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

Homeland Security

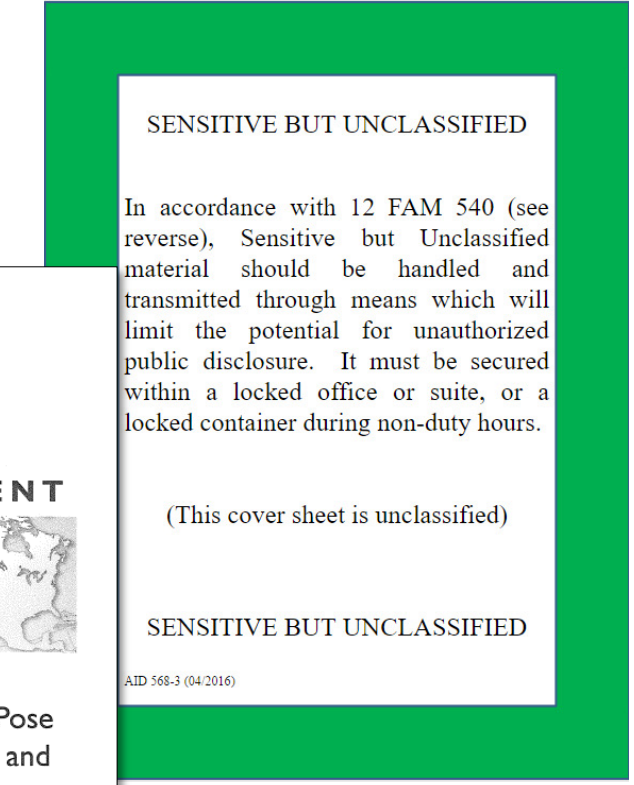
INTELLIGENCE ASSESSMENT

(U//FOUO) Domestic Violent Extremists Pose Increased Threat to Government Officials and Law Enforcement

22 July 2014

Office of Intelligence and Analysis
IA-0201-14

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

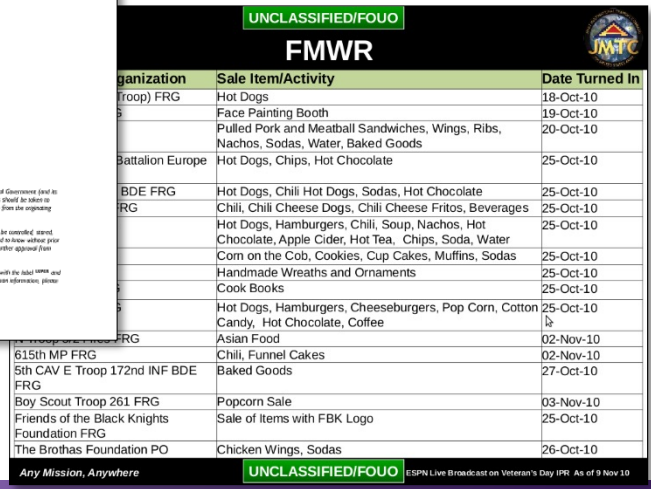

SENSITIVE BUT UNCLASSIFIED

In accordance with 12 FAM 540 (see reverse), Sensitive but Unclassified material should be handled and transmitted through means which will limit the potential for unauthorized public disclosure. It must be secured within a locked office or suite, or a locked container during non-duty hours.

(This cover sheet is unclassified)

SENSITIVE BUT UNCLASSIFIED

AID 568-3 (04/2016)


UNCLASSIFIED/FOUO

FMWR

ganization	Sale Item/Activity	Date Turned In
Troop) FRG	Hot Dogs	18-Oct-10
5	Face Painting Booth	19-Oct-10
	Pulled Pork and Meatball Sandwiches, Wings, Ribs, Nachos, Sodas, Water, Baked Goods	20-Oct-10
Battalion Europe	Hot Dogs, Chips, Hot Chocolate	25-Oct-10
BDE FRG	Hot Dogs, Chili Hot Dogs, Sodas, Hot Chocolate	25-Oct-10
RG	Chili, Chili Cheese Dogs, Chili Cheese Fritos, Beverages	25-Oct-10
	Hot Dogs, Hamburgers, Chili, Soup, Nachos, Hot Chocolate, Apple Cider, Hot Tea, Chips, Soda, Water	25-Oct-10
	Corn on the Cob, Cookies, Cup Cakes, Muffins, Sodas	25-Oct-10
	Handmade Wreaths and Ornaments	25-Oct-10
	Cook Books	25-Oct-10
5	Hot Dogs, Hamburgers, Cheeseburgers, Pop Corn, Cotton Candy, Hot Chocolate, Coffee	25-Oct-10
RG	Asian Food	02-Nov-10
615th MP FRG	Chili, Funnel Cakes	02-Nov-10
5th CAV E Troop 172nd INF BDE FRG	Baked Goods	27-Oct-10
Boy Scout Troop 261 FRG	Popcorn Sale	03-Nov-10
Friends of the Black Knights Foundation FRG	Sale of Items with FBK Logo	25-Oct-10
The Brothas Foundation PO	Chicken Wings, Sodas	26-Oct-10

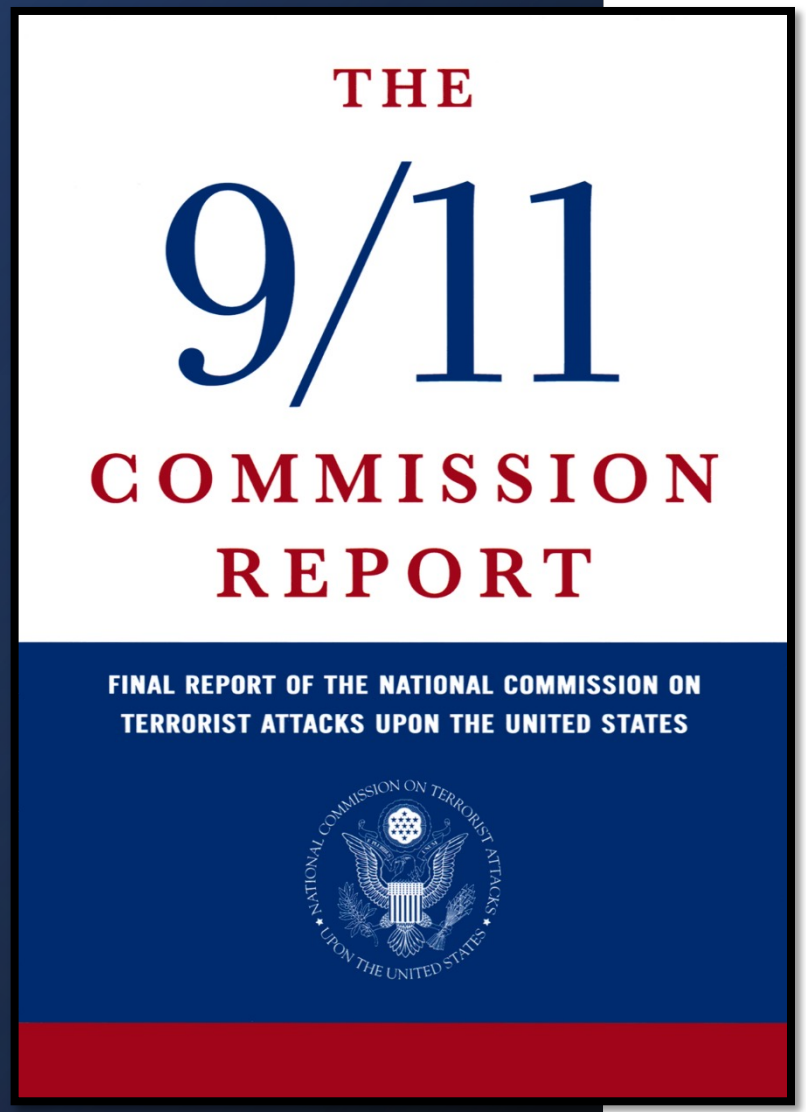
Any Mission, Anywhere UNCLASSIFIED/FOUO ESPN Live Broadcast on Veteran's Day IPR As of 9 Nov 10

Inconsistent Approaches

- Agency A FOUO Policy:
  - Cannot be disseminated outside the agency (not even to contractors)
  - Must only be sent via USPS
  - All envelopes containing FOUO must be conspicuously marked
- Agency B FOUO Policy:
  - Cannot be disseminated outside the agency except to contractors
  - May be sent via USPS, UPS, or FedEx but not by courier
  - Envelopes containing FOUO must be indistinguishable from other mail

Inconsistency Led to Distrust

- Agency A doesn't trust Agency B because Agency B "mishandled" FOUO
  - Government contractors who work for multiple agencies struggle with how to properly identify and handle information.
- Led to:
  - information silos and
  - a feeling of information "ownership"
    - despite the collection/creation of that information having been taxpayer-funded.

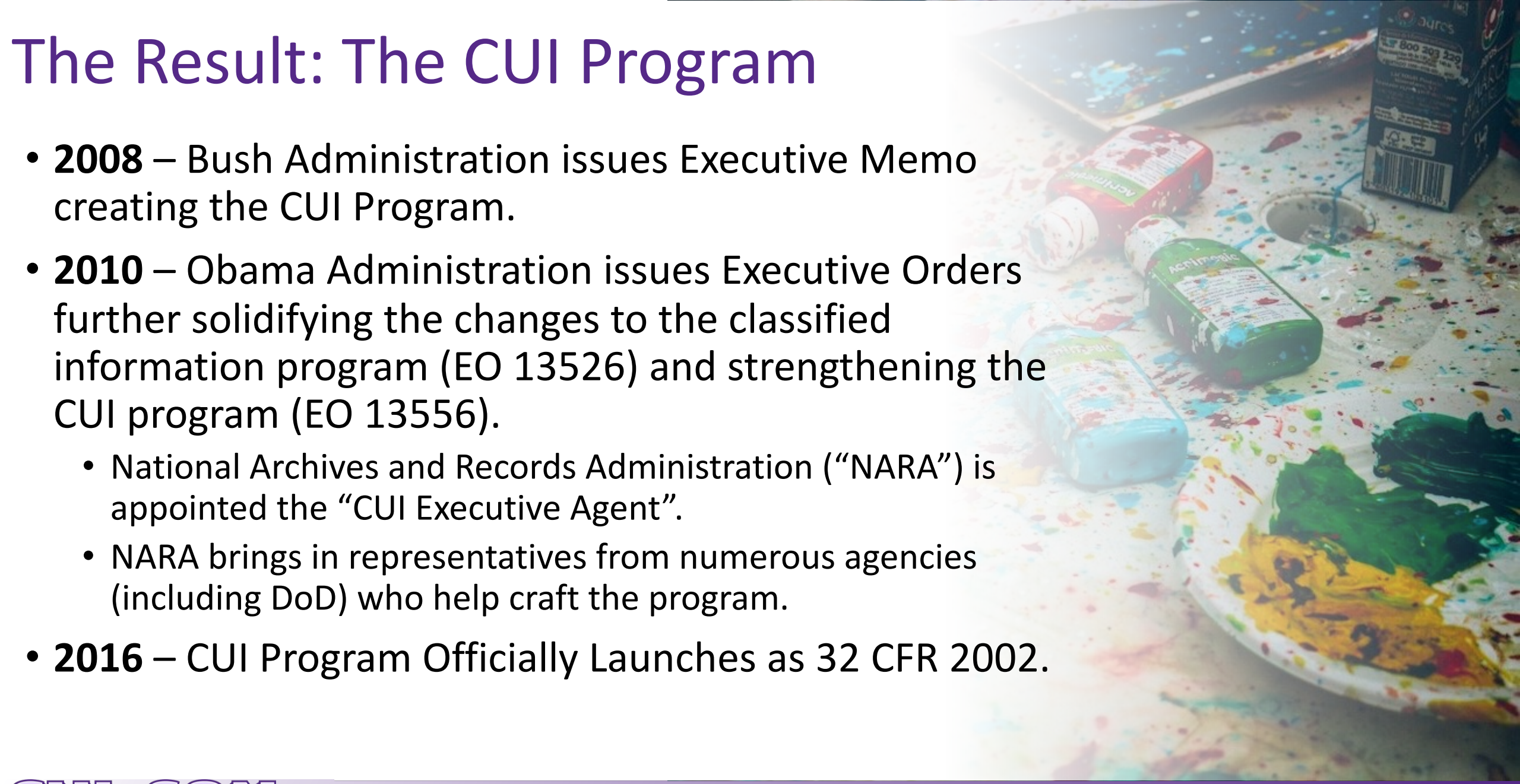


Distrust Leads to Catastrophic Impact on U.S. National Security

- Agencies had the information needed to identify and catch the 9/11 terrorists.
- Agency reluctance to share information allowed the terrorists to complete their acts.
- The Federal Government needed a new approach to identifying and protecting sensitive information.
- That approach must:
  - be consistent across the entire federal government
  - Recognize that unclassified information is unclassified and treat it as such
  - encourage information sharing to authorized persons (get away from “need to know” mindset)

The Result: The CUI Program

- **2008** – Bush Administration issues Executive Memo creating the CUI Program.
- **2010** – Obama Administration issues Executive Orders further solidifying the changes to the classified information program (EO 13526) and strengthening the CUI program (EO 13556).
  - National Archives and Records Administration (“NARA”) is appointed the “CUI Executive Agent”.
  - NARA brings in representatives from numerous agencies (including DoD) who help craft the program.
- **2016** – CUI Program Officially Launches as 32 CFR 2002.



Controlled Unclassified Information

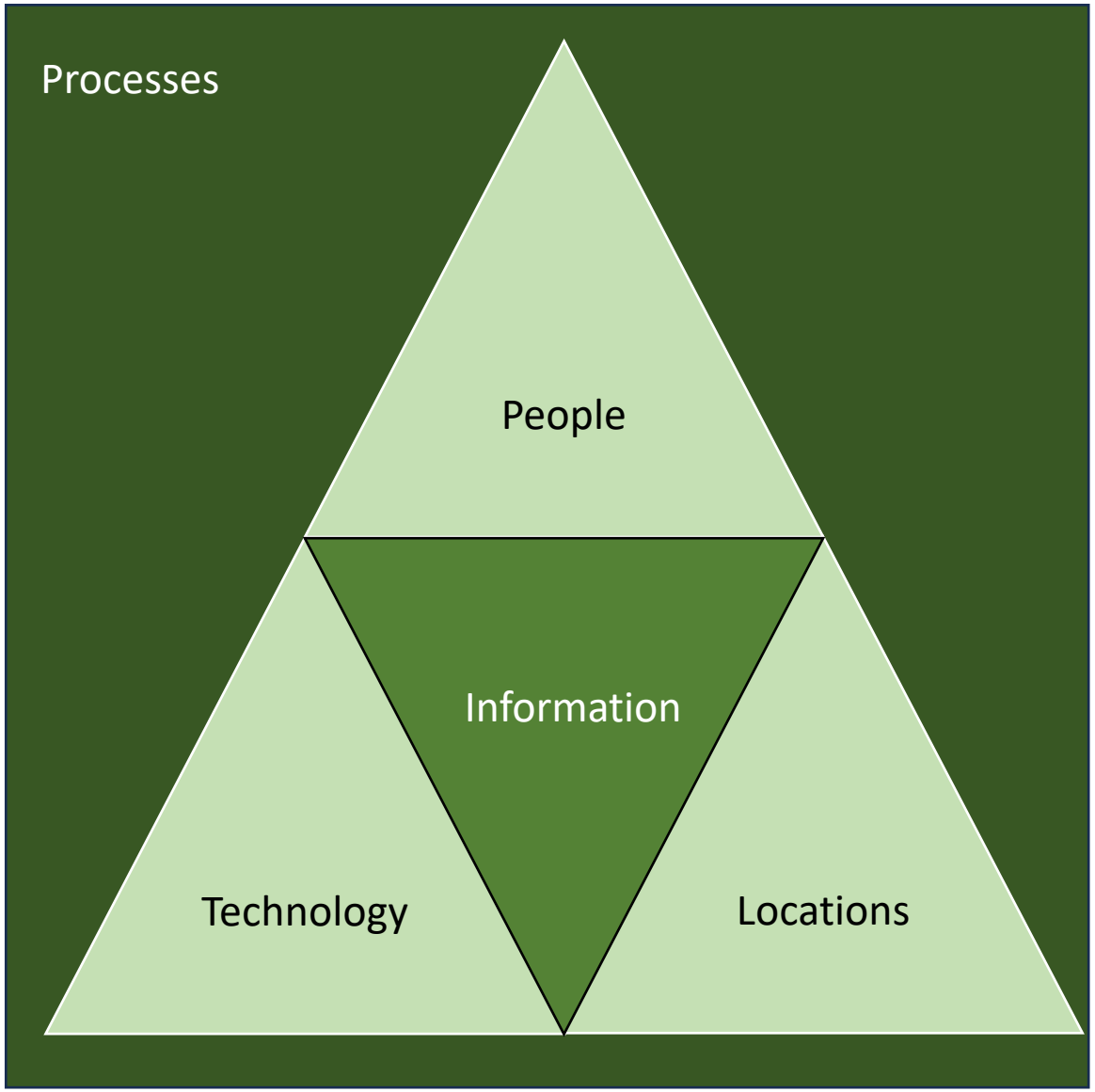
- unclassified information;
- created or possessed by or on behalf of the Government; **AND**
- there **must** be a **law, regulation, or government-wide policy** ("LRGWP") that requires or permits the information to be either:
  - safeguarded or
  - subject to dissemination controls **AND**
- the LRGWP **must** be listed in the NARA CUI Registry (https://Archives.gov/CUI)

CUI Specified and CUI Basic

- If the LRGWP includes specific safeguarding requirements or dissemination controls, that makes the covered information "**CUI Specified**".
- If the LRGWP simply requires safeguarding, the information is "**CUI Basic**".

NARA to Agencies: This is the way to Safeguard CUI Basic

- Agencies must safeguard CUI in accordance with FIPS PUB 199, FIPS PUB 200, and NIST SP 800-53.
- NARA realized that this is too much to ask of contractors. They asked NIST to conduct a risk assessment and create a standard set of “reasonable” requirements for contractors who handle CUI. NIST SP 800-171 is the result.
- Agencies must use NIST SP 800-171 when establishing security requirements to protect CUI’s confidentiality in non-federal systems.
- CUI Specified is safeguarded as CUI Basic + specific requirements in the LRGWP.



800-171 in a Nutshell:

- Identify the:
  - CUI you have;
  - Locations where the CUI is handled;
  - People who have access to the CUI;
  - Technology used in handling the CUI; and,
  - Processes that govern those locations, people, and technology.
    - Policies
    - Procedures
    - Plans
    - Other documentation
- Ensure these all comply with the 110 requirements in NIST SP 800-171, as further refined in the 320 objectives in NIST SP 800-171A.

2016:
DoD Blazes a Trail

- DoD begins implementing CUI program internally.
- DoD rolls out DFARS 252.204-7012 to contractors.
  - Defines “Covered Defense Information” and “Controlled Technical Information” as forms of CUI.
  - Requires contractors to safeguard CUI in accordance with NIST SP 800-171.
  - Effective beginning in 2017.
- Contractors begin self-attesting to compliance by entering into contracts containing the -7012 clause.
  - Did they read it, or even notice its addition?

DoD Realized there is a Problem

- Hard Lesson Learned: when DoD gives contractors CUI, contractors aren't safeguarding it.
  - **2018 -** DoD Inspector General Report shows contractors are not meeting the NIST SP 800-171 requirements.
  - **2019 –** DIBCAC's independent assessments show that contractors are not meeting the NIST SP 800-171 requirements.
- This results in:
  - basic legal risk exposure for the government
  - increased Congressional scrutiny
  - exfiltration of sensitive information to our adversaries

Real-world Risks

- The exfiltration of DoD's sensitive CUI puts our warfighters in danger
  - Technology
    - Create "clones" of the tools used by our service members w/o R&D expense
    - Probe for weaknesses
  - PII/PHI
    - Influence by foreign governments
    - Targeting of family members
    - Distraction while deployed

DoD's Solution: The CMMC Program

- Majority of contractors who handle CUI must obtain a certification of compliance with NIST SP 800-171 requirements.
- Certifications are issued by third-parties (Certified 3rd Party Assessment Organizations ("C3PAOs") or DIBCAC).
- Certifications are issued after an assessment conducted by an assessment team.
- Assessment team validates your own internal assessment and attestation of compliance.

What is Assed? Evidence

- **Examine** – Documentary evidence that describes the organization's business practices and how those practices enable the organization to meet all of the requirements/objectives.
- **Interview** – Discussions with the people who handle the implementation of the business practices to ensure what they do aligns with what is in the documentary evidence.
- **Test** – Shoulder surfing (or other evidence) that demonstrates that the organization is actually doing what is written in the documentation and what the staff said is being done.

Collecting and Organizing Evidence

- Assessors won't accept a "data dump."
- You need to do the diligence. The assessors are validating your attestation of compliance.
- Assessors expect to see a "traceability matrix" that shows how and where each piece of evidence is relevant for a given requirement/objective.
- Can be achieved in a number of ways, including:
  - Spreadsheets and File Folders
  - General Purpose Tools
  - Purpose-built Tools
- When choosing a tool, look for:
  - NIST SP 800-171 **including NIST SP 800-171A objectives**
  - Creation and management of POA&Ms
  - Easy export of your information to common formats

CMMC Certifications

- Issued by the C3PAO (or DIBCAC) upon satisfactory demonstration of compliance with the requirements.
- Conditional Certifications
  - Minimum score (88) is required for conditional certification
  - Certain requirements must be met
  - All gaps must be remediated, and their corresponding POA&Ms closed, within 180 days
- "Final" certification
  - issued once all POA&Ms are demonstrated to be closed
  - valid for 3 years
- Contractors must submit an attestation of their compliance annually (including the first year).

Self Assessments when Handling CUI

- Don't count on them.
  - 82,085 contractors are expected to handle CUI.
  - 78,085 (95%) contractors are expected to need CMMC certifications from C3PAOs.
  - Only 4,000 (5%) contractors are expected to handle CUI but won't need certifications.
- Full self-assessment every 3 years (triennial)
- Annual affirmation of continuing compliance.
- Contracting officers have the latitude to award based on the distinction between self-assessed and certified environments.

CMMC: More than just CUI

- Even though information doesn't meet the sensitive/CUI definition, that doesn't mean it should be plastered across the Internet.
  - e.g.: Private E-mails/Text messages that don't contain CUI
- That unclassified, uncontrolled, non-public information is referred to as Federal Contract Information ("FCI") when given to/created by contractors under a contract.
- CMMC Level 1 focuses on the protection of FCI.
  - 139,201 contractors expected to "only" need to comply with CMMC Level 1
  - FAR 52.204-21 defines the 15 safeguarding requirements
  - Self-assessments and attestations
- **NOTE:** FCI and CUI may have very different assessment "scopes"

Why the Fixation on CUI and CMMC Level 2 Certifications?

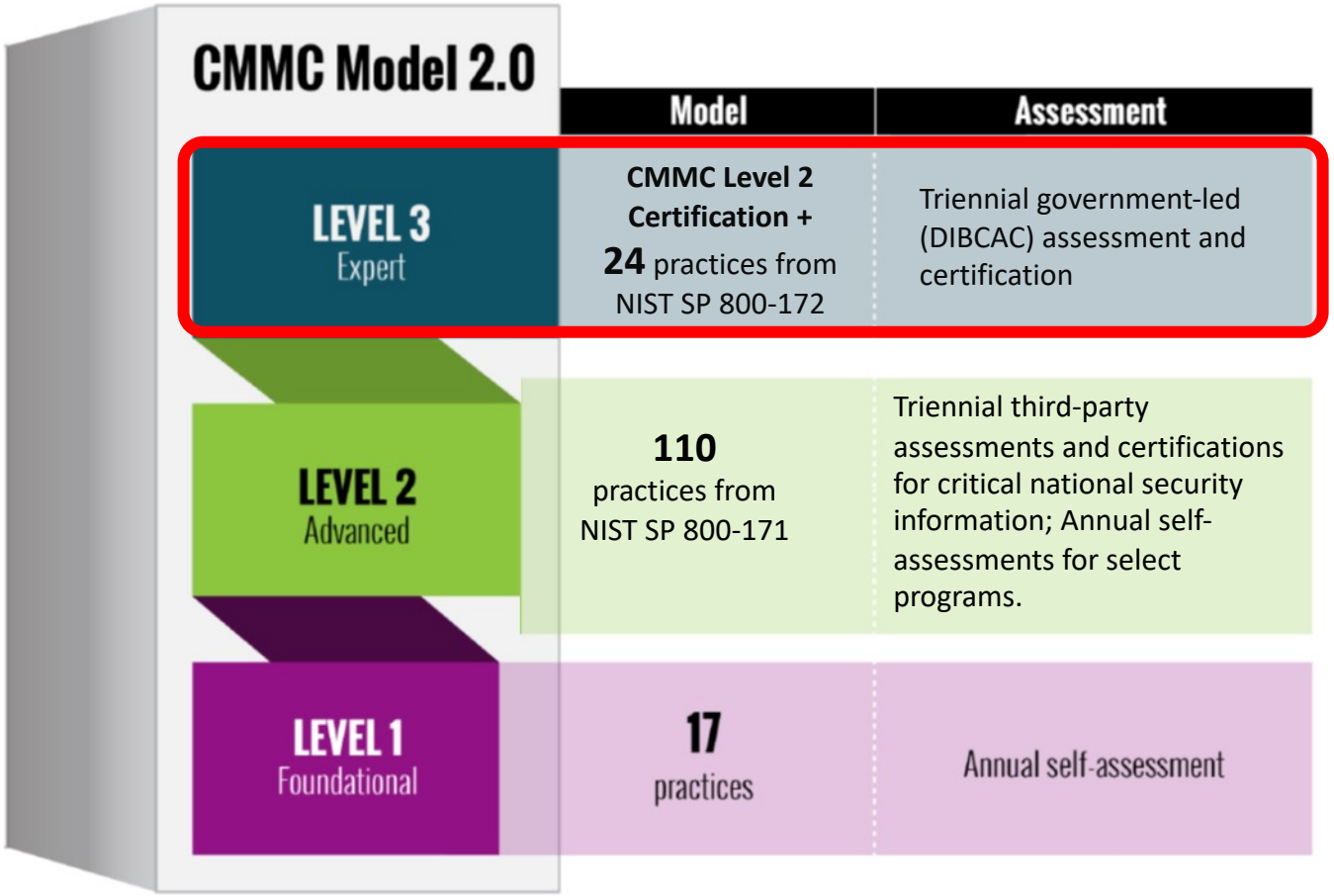
- In a word:

Efficiency

- The CUI program is a fundamental transformation of the way the government handles information.
- It requires “unlearning” decades of established practices. That takes a LONG time in big orgs.
- Federal agencies are still learning the difference between CUI designation and marking, and how to do them properly.
- Prime contractors are not confident that the information they handle will be properly marked.
- To avoid unintentionally “spilling” CUI, it is easier for them to focus on contracting with companies that are CMMC Level 2 certified.

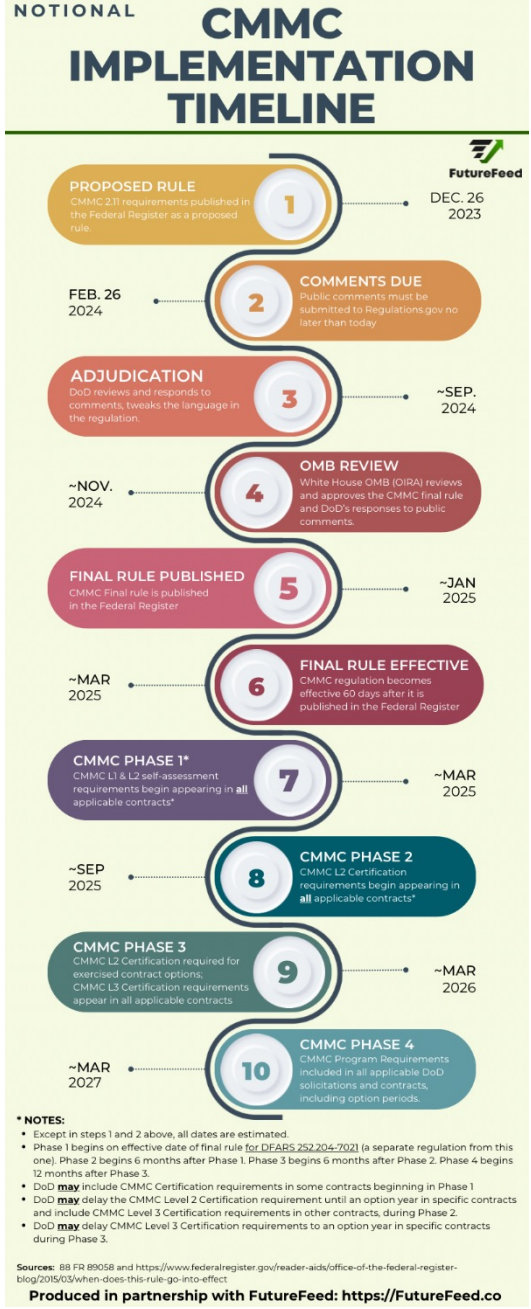
And Then There's Level 3…

- 1,487 contractors are expected to need CMMC Level 3 (1%).
- Must have a CMMC Level 2 certification for that environment first.
- DIBCAC performs an assessment of 24 requirements from NIST SP 800-172 and issues a separate CMMC Level 3 certification.
- We don't yet know what will trigger a CMMC Level 3 Certification requirement.



Where are We Now?

- DoD published 32 CFR 170 as a Notice of Proposed Rulemaking ("NPRM") on 2023-DEC-26.
- 32 CFR 170 is a set of regulations which define the CMMC program.
- DoD must accept public comments on 32 CFR 170 until Feb. 26.
- DoD must adjudicate the comments and make appropriate changes to 32 CFR 170.
- DoD must publish this as a "final" version of 32 CFR 170.
- The final rule will go into effect approx. 60 days after it is published.
- That rule is expected to publish in late CY2024 or early 2025.
- 4-phase roll-out to CMMC. CY2027 for full implementation, **BUT** contractors could start to see self-assessment requirements in 2025 and certification requirements in late 2025 or early 2026 **and maybe sooner**.



But wait…there's more!

- There are two other CMMC-related rules that are working their way through the regulatory review and approval process.
  - Changes to DFARS 252.204-7012 [2023-D021] which:
    - Will codify some of the CMMC Level 3 requirements (i.e., make portions of NIST SP 800-172 a requirement)
    - Also expected to refine the FedRAMP requirements for cloud services, to delineate, consistent with 32 CFR 170, the differences between CSPs and ESPs and more.
  - Changes to DFARS 252.204-7021 [2022-D017] to make those requirements consistent with 32 CFR 170.
- These are expected to be published soon (currently late March).
- CMMC will not fully go into effect until the changes to DFARS 252.204-7021 are final.
- This is expected to be coordinated with the finalization of 32 CFR 170.

Summary

- Like commercial entities, the government must protect sensitive information.
- The government refers to its unclassified, sensitive information as CUI.
- Contractors must protect CUI by fully implementing the requirements in NIST SP 800-171.
- DoD tried simply asking contractors to comply; that didn't work out so well.
- DoD is now requiring third-party certification of compliance for most contractors who handle CUI. This is CMMC.
- All contractors, including those who only handle FCI, will have to do annual compliance affirmations.
- NIST SP800-171 defines "reasonable care" for the government's sensitive information. This makes it a good foundation for all cyber programs, especially those involving sensitive information.
- Don't wait. CMMC will likely show up in contracts in 12-18 months, but implementation can take that long, or longer.
- Primes aren't waiting that long and won't wait for you to get CMMC certified.

Coming Up

- LOTS of great sessions that will explore these and related concepts in more detail, including:
  - Applying these concepts to your supply chain
  - How your MSP/MSSP ties into all of this
  - How cloud service providers are dealing with, and helping you prepare for, CMMC
  - Scoping
  - Common pitfalls
  - Dealing with Operational Technology (“OT”)
  - Simulated Assessments and C3PAO Panels

Overmarking

- Designating information as “sensitive” when it shouldn’t be.
- There needs to be a well-defined basis for when information is “sensitive”
- Can’t use “sensitive” as an excuse to hide negligence, ineptitude or other disreputable circumstances embarrassing to a person, an agency, or the government

UNCLASSIFIED/FOUO

U.S. ARMY EUROPE

FMWR

JMTC

FRG/Private Organization	Sale Item/Activity	Date Turned In
2 SCR RSS (S&T Troop) FRG	Hot Dogs	18-Oct-10
3-66 AR A Co FRG	Face Painting Booth	19-Oct-10
1-2 IN HHC FRG	Pulled Pork and Meatball Sandwiches, Wings, Ribs, Nachos, Sodas, Water, Baked Goods	20-Oct-10
Warrior Transition Battalion Europe D Co FRG	Hot Dogs, Chips, Hot Chocolate	25-Oct-10
57th Sig, 172nd IN BDE FRG	Hot Dogs, Chili Hot Dogs, Sodas, Hot Chocolate	25-Oct-10
172nd BDE HHC FRG	Chili, Chili Cheese Dogs, Chili Cheese Fritos, Beverages	25-Oct-10
2-28 IN B Co FRG	Hot Dogs, Hamburgers, Chili, Soup, Nachos, Hot Chocolate, Apple Cider, Hot Tea, Chips, Soda, Water	25-Oct-10
2-28 IN C Co FRG	Corn on the Cob, Cookies, Cup Cakes, Muffins, Sodas	25-Oct-10
1-2 IN A Co FRG	Handmade Wreaths and Ornaments	25-Oct-10
3-66 AR B Co FRG	Cook Books	25-Oct-10
4-319th AFAR FRG	Hot Dogs, Hamburgers, Cheeseburgers, Pop Corn, Cotton Candy, Hot Chocolate, Coffee	25-Oct-10
N Troop 5/2 Fires FRG	Asian Food	02-Nov-10
615th MP FRG	Chili, Funnel Cakes	02-Nov-10
5th CAV E Troop 172nd INF BDE FRG	Baked Goods	27-Oct-10
Boy Scout Troop 261 FRG	Popcorn Sale	03-Nov-10
Friends of the Black Knights Foundation FRG	Sale of Items with FBK Logo	25-Oct-10
The Brothas Foundation PO	Chicken Wings, Sodas	26-Oct-10

Any Mission, Anywhere

UNCLASSIFIED/FOUO

ESPN Live Broadcast on Veteran’s Day IPR As of 9 Nov 10