Stay Informed and Follow Us

SAME

Fort Worth Post

Website
www.samefortworth.org

Instagram
@same_fortworth

LinkedIn
Society of American Military Engineers
Fort Worth Post

Facebook
Society of American Military Engineers
Fort Worth Post

CMMC Briefing

SAME, Fort Worth

Dean Rock
CEO, SteelToad Consulting LLC

September 7, 2022

STEELTOAD

TECHNICAL SOLUTIONS PROVIDER

SteelToad Technical Solutions Provider

Dean Rock
CEO

STEELTOAD
TECHNICAL SOLUTIONS PROVIDER

Professional Experience:

CIO/Service Delivery/ Technical Solutions in Business Development

25 years of Solution delivery to federal government.

State Department, DHS, Treasury, USA Today, Oracle, Sybase, Department of Defense Cyber Crime Center (DC3), Navy, Charter Communications

Certifications

CMMI, Cyber Security CMMC Provisional Instructor, CMMC Assessor,
ISO LA ISC CISSP, ISACA CISA and CISM security certifications Oracle, IBM DB2, Microsoft.

Designations:

SCRUM Master, CMMI Trainer, CMMI Lead Appraiser Development, Services, Supplier Management, Data Management (EDME), Medical Devices, ISO 9001, 27000, 20000, 13485 CMMI Enterprise Data Management Expert, UMUC Adjunct Professor – Adv. Database Concepts

CYBERSECURITY MATURITY MODEL CERTIFICATION CMMC-AB C3PAO AUTHORIZED

CYBERSECURITY MATURITY MODEL CERTIFICATION CMMC-AB LTP LICENSED

CMMC–AB PROVISIONAL ASSESSOR

CMMC–AB PROVISIONAL INSTRUCTOR

ISACA ACCREDITED PARTNER CISA CISM

HUBZone Historically Underutilized Business Zone CERTIFIED

CMMI® Institute Partner

CMMC Briefing

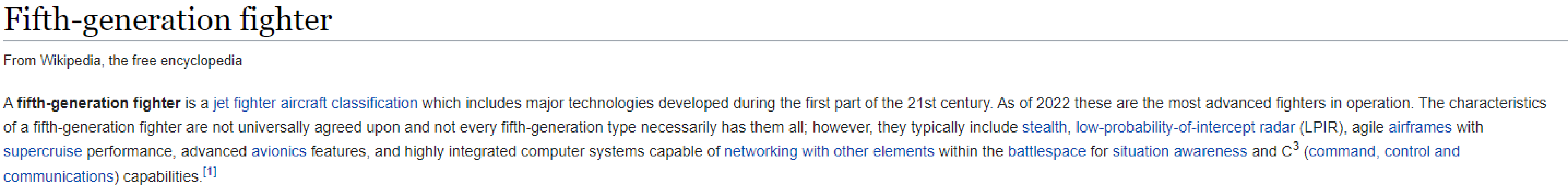
- Discuss CMMC Certification.
- Update on the current guidance and regs for achieving certification.
- Explain the requirements based on sensitivity of data.
- Discuss timeframe for CMMC.
- Typical outcomes or issues that firms need to address to become certified.

WHY CMMC?

Protection of Critical Data

- **US F-35**
  - 5th generation strike/fighter aircraft
  - Super cruise (supersonic)
  - High-tech platform – sensor to weapon system
  - Costs: $94-122M per plane
    - Estimated $1.5T over course of 55-year period

- **Chinese J-31**
  - China stole (CTI) data from multiple contractors.
  - Perform production/product integration.
  - Saved time, money, R&D to develop prototype.
    - Monetary savings used to further hurt U.S. businesses (e.g., drive down product prices).



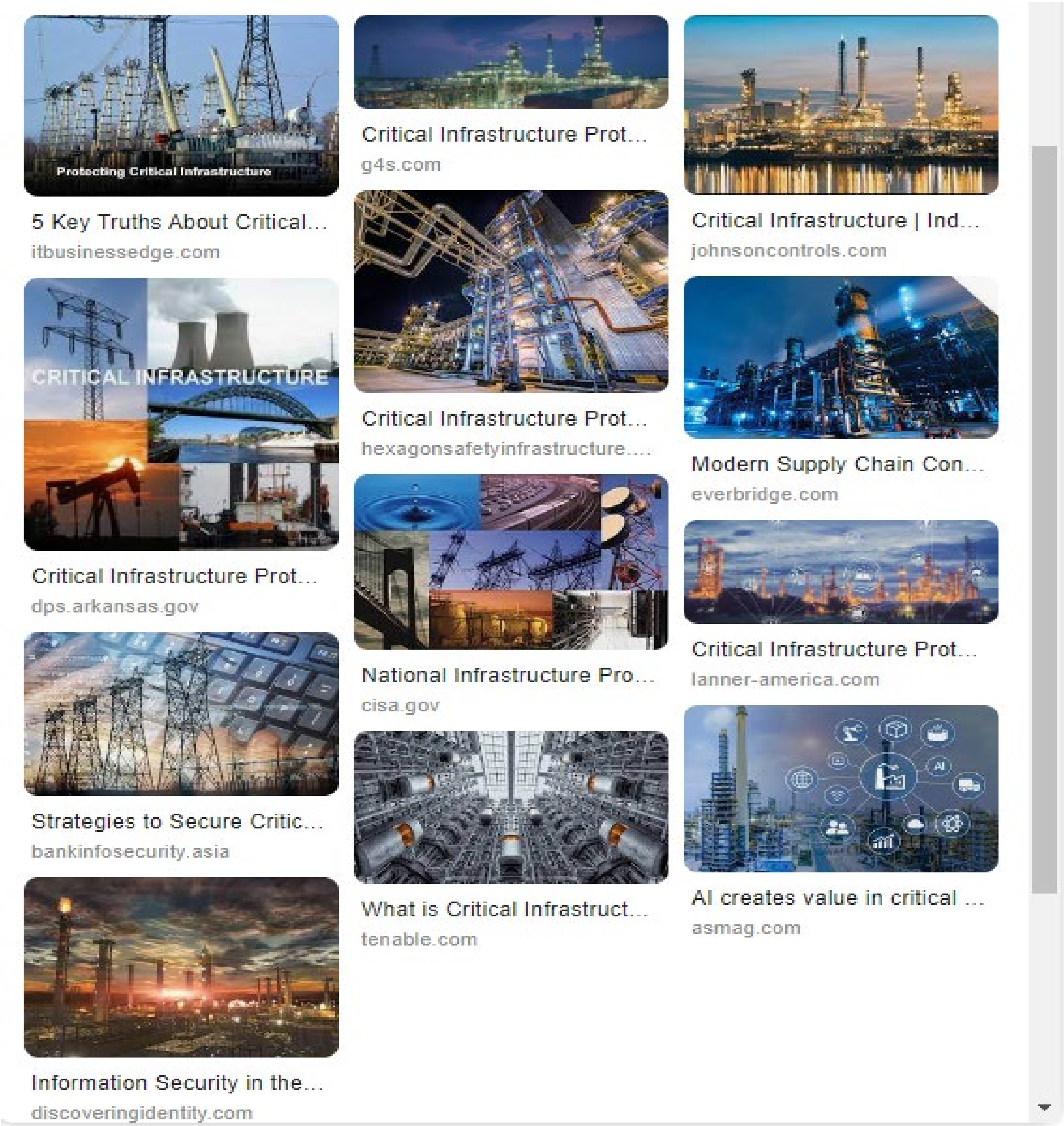
Fifth-generation fighter

From Wikipedia, the free encyclopedia

A **fifth-generation fighter** is a jet fighter aircraft classification which includes major technologies developed during the first part of the 21st century. As of 2022 these are the most advanced fighters in operation. The characteristics of a fifth-generation fighter are not universally agreed upon and not every fifth-generation type necessarily has them all; however, they typically include stealth, low-probability-of-intercept radar (LPIR), agile airframes with supercruise performance, advanced avionics features, and highly integrated computer systems capable of networking with other elements within the battlespace for situation awareness and C^3 (command, control and communications) capabilities.[1]

WHY CMMC?

Protection of Critical Infrastructure Data



5 Key Truths About Critical...
itbusinessedge.com

Critical Infrastructure Prot...
dps.arkansas.gov

Strategies to Secure Critic...
bankinfosecurity.asia

Information Security in the...
discoveringidentity.com

Critical Infrastructure Prot...
g4s.com

Critical Infrastructure Prot...
hexagonsafetyinfrastructure....

National Infrastructure Pro...
cisa.gov

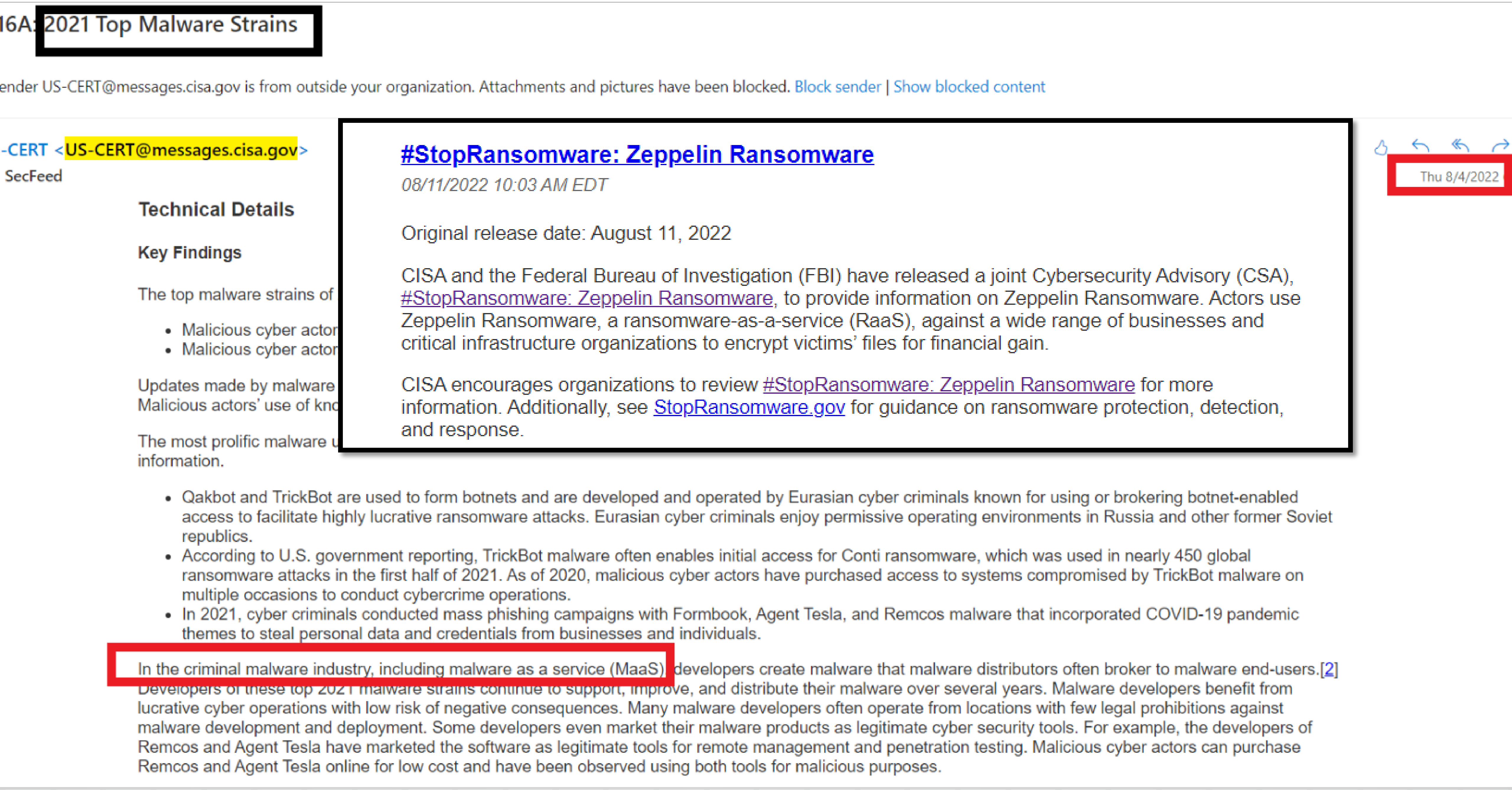
What is Critical Infrastruct...
tenable.com

Critical Infrastructure | Ind...
johnsoncontrols.com

Modern Supply Chain Con...
everbridge.com

Critical Infrastructure Prot...
lanner-america.com

AI creates value in critical ...
asmag.com



16A: 2021 Top Malware Strains

ender US-CERT@messages.cisa.gov is from outside your organization. Attachments and pictures have been blocked. Block sender | Show blocked content

-CERT <US-CERT@messages.cisa.gov>

SecFeed

Thu 8/4/2022

[#StopRansomware: Zeppelin Ransomware](#)

08/11/2022 10:03 AM EDT

Original release date: August 11, 2022

CISA and the Federal Bureau of Investigation (FBI) have released a joint Cybersecurity Advisory (CSA), #StopRansomware: Zeppelin Ransomware, to provide information on Zeppelin Ransomware. Actors use Zeppelin Ransomware, a ransomware-as-a-service (RaaS), against a wide range of businesses and critical infrastructure organizations to encrypt victims' files for financial gain.

CISA encourages organizations to review #StopRansomware: Zeppelin Ransomware for more information. Additionally, see StopRansomware.gov for guidance on ransomware protection, detection, and response.

Technical Details

Key Findings

The top malware strains of

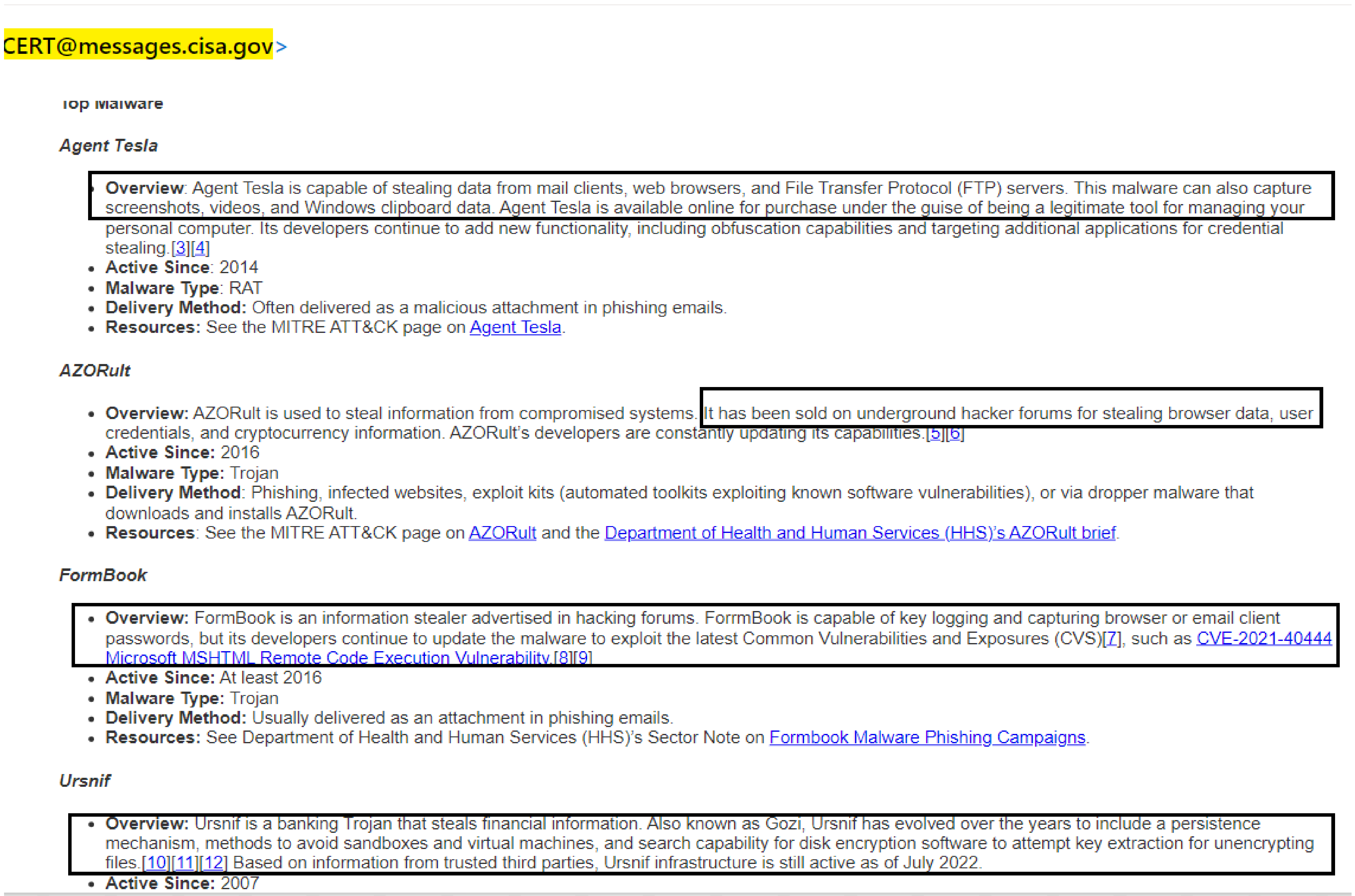
- Malicious cyber actor
- Malicious cyber actor

Updates made by malware
Malicious actors' use of kno

The most prolific malware u
information.

- Qakbot and TrickBot are used to form botnets and are developed and operated by Eurasian cyber criminals known for using or brokering botnet-enabled access to facilitate highly lucrative ransomware attacks. Eurasian cyber criminals enjoy permissive operating environments in Russia and other former Soviet republics.
- According to U.S. government reporting, TrickBot malware often enables initial access for Conti ransomware, which was used in nearly 450 global ransomware attacks in the first half of 2021. As of 2020, malicious cyber actors have purchased access to systems compromised by TrickBot malware on multiple occasions to conduct cybercrime operations.
- In 2021, cyber criminals conducted mass phishing campaigns with Formbook, Agent Tesla, and Remcos malware that incorporated COVID-19 pandemic themes to steal personal data and credentials from businesses and individuals.

In the criminal malware industry, including malware as a service (MaaS) developers create malware that malware distributors often broker to malware end-users.[2] Developers of these top 2021 malware strains continue to support, improve, and distribute their malware over several years. Malware developers benefit from lucrative cyber operations with low risk of negative consequences. Many malware developers often operate from locations with few legal prohibitions against malware development and deployment. Some developers even market their malware products as legitimate cyber security tools. For example, the developers of Remcos and Agent Tesla have marketed the software as legitimate tools for remote management and penetration testing. Malicious cyber actors can purchase Remcos and Agent Tesla online for low cost and have been observed using both tools for malicious purposes.



CERT@messages.cisa.gov>

Top Malware

Agent Tesla

- **Overview**: Agent Tesla is capable of stealing data from mail clients, web browsers, and File Transfer Protocol (FTP) servers. This malware can also capture screenshots, videos, and Windows clipboard data. Agent Tesla is available online for purchase under the guise of being a legitimate tool for managing your personal computer. Its developers continue to add new functionality, including obfuscation capabilities and targeting additional applications for credential stealing.[3][4]
- **Active Since**: 2014
- **Malware Type**: RAT
- **Delivery Method:** Often delivered as a malicious attachment in phishing emails.
- **Resources:** See the MITRE ATT&CK page on Agent Tesla.

AZORult

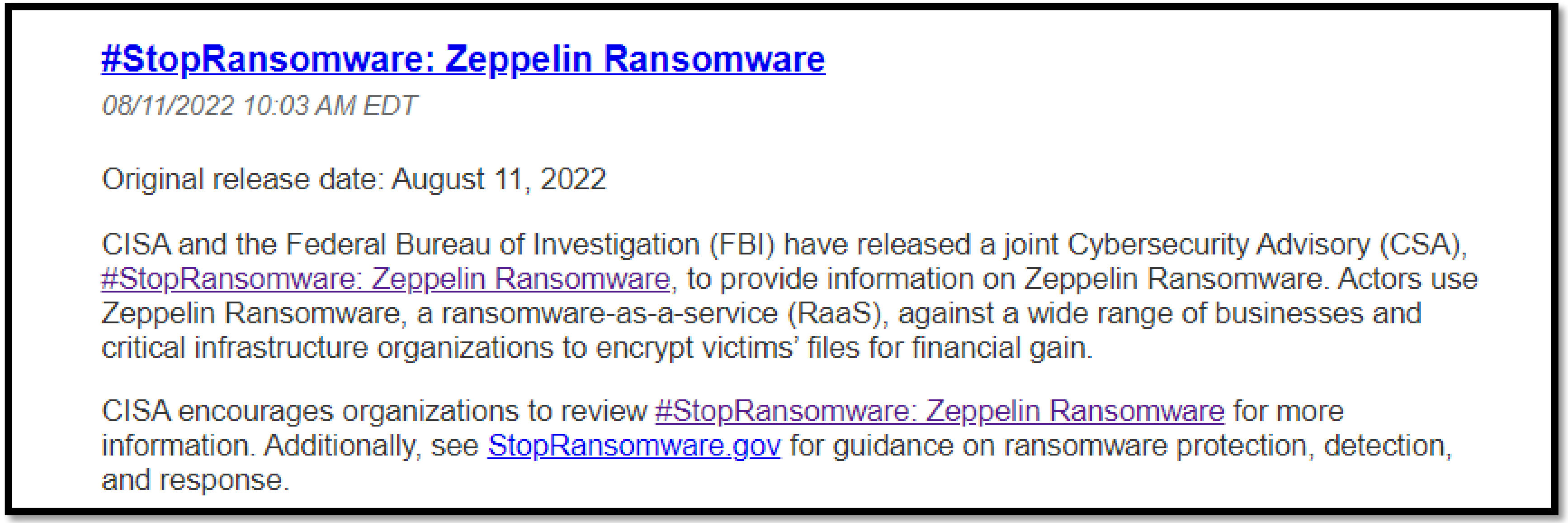
- **Overview:** AZORult is used to steal information from compromised systems. It has been sold on underground hacker forums for stealing browser data, user credentials, and cryptocurrency information. AZORult's developers are constantly updating its capabilities.[5][6]
- **Active Since:** 2016
- **Malware Type:** Trojan
- **Delivery Method**: Phishing, infected websites, exploit kits (automated toolkits exploiting known software vulnerabilities), or via dropper malware that downloads and installs AZORult.
- **Resources**: See the MITRE ATT&CK page on AZORult and the Department of Health and Human Services (HHS)'s AZORult brief.

FormBook

- **Overview:** FormBook is an information stealer advertised in hacking forums. FormmBook is capable of key logging and capturing browser or email client passwords, but its developers continue to update the malware to exploit the latest Common Vulnerabilities and Exposures (CVS)[7], such as CVE-2021-40444 Microsoft MSHTML Remote Code Execution Vulnerability.[8][9]
- **Active Since:** At least 2016
- **Malware Type:** Trojan
- **Delivery Method:** Usually delivered as an attachment in phishing emails.
- **Resources:** See Department of Health and Human Services (HHS)'s Sector Note on Formbook Malware Phishing Campaigns.

Ursnif

- **Overview:** Ursnif is a banking Trojan that steals financial information. Also known as Gozi, Ursnif has evolved over the years to include a persistence mechanism, methods to avoid sandboxes and virtual machines, and search capability for disk encryption software to attempt key extraction for unencrypting files.[10][11][12] Based on information from trusted third parties, Ursnif infrastructure is still active as of July 2022.
- **Active Since:** 2007



#StopRansomware: Zeppelin Ransomware

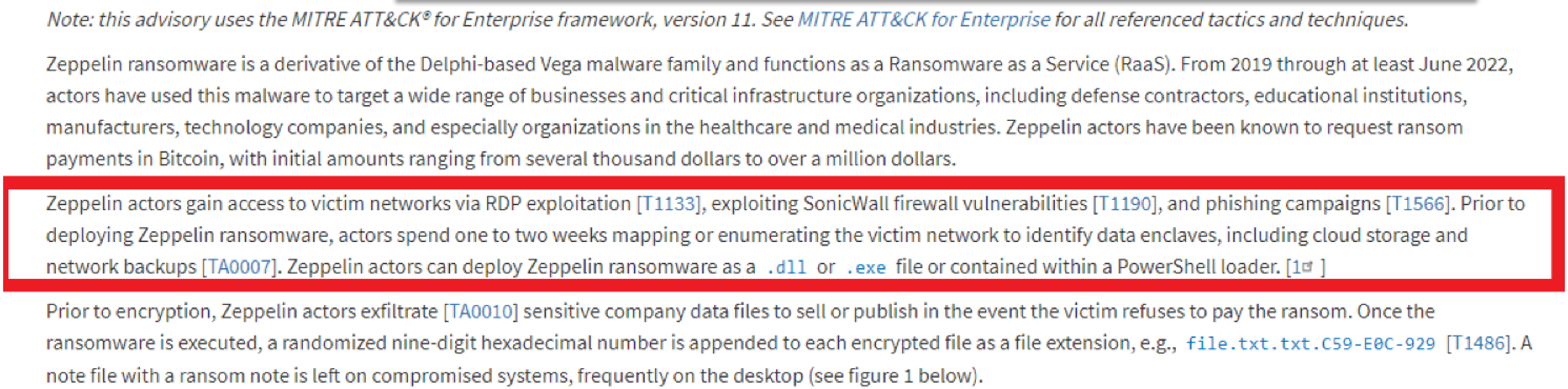
08/11/2022 10:03 AM EDT

Original release date: August 11, 2022

CISA and the Federal Bureau of Investigation (FBI) have released a joint Cybersecurity Advisory (CSA), #StopRansomware: Zeppelin Ransomware, to provide information on Zeppelin Ransomware. Actors use Zeppelin Ransomware, a ransomware-as-a-service (RaaS), against a wide range of businesses and critical infrastructure organizations to encrypt victims' files for financial gain.

CISA encourages organizations to review #StopRansomware: Zeppelin Ransomware for more information. Additionally, see StopRansomware.gov for guidance on ransomware protection, detection, and response.

Technical Details



Note: this advisory uses the MITRE ATT&CK® for Enterprise framework, version 11. See MITRE ATT&CK for Enterprise for all referenced tactics and techniques.

Zeppelin ransomware is a derivative of the Delphi-based Vega malware family and functions as a Ransomware as a Service (RaaS). From 2019 through at least June 2022, actors have used this malware to target a wide range of businesses and critical infrastructure organizations, including defense contractors, educational institutions, manufacturers, technology companies, and especially organizations in the healthcare and medical industries. Zeppelin actors have been known to request ransom payments in Bitcoin, with initial amounts ranging from several thousand dollars to over a million dollars.

Zeppelin actors gain access to victim networks via RDP exploitation [T1133], exploiting SonicWall firewall vulnerabilities [T1190], and phishing campaigns [T1566]. Prior to deploying Zeppelin ransomware, actors spend one to two weeks mapping or enumerating the victim network to identify data enclaves, including cloud storage and network backups [TA0007]. Zeppelin actors can deploy Zeppelin ransomware as a `.dll` or `.exe` file or contained within a PowerShell loader. [1]

Prior to encryption, Zeppelin actors exfiltrate [TA0010] sensitive company data files to sell or publish in the event the victim refuses to pay the ransom. Once the ransomware is executed, a randomized nine-digit hexadecimal number is appended to each encrypted file as a file extension, e.g., `file.txt.txt.C59-E0C-929` [T1486]. A note file with a ransom note is left on compromised systems, frequently on the desktop (see figure 1 below).

What type of data do you need to protect?

Executive Order 13556, Controlled Unclassified Information (**EO 13556)**

Unclassified Information

- Standardized handling of protected information
- Subject to laws governing data of data
- What does your contract state?

National Archives and Records Administration

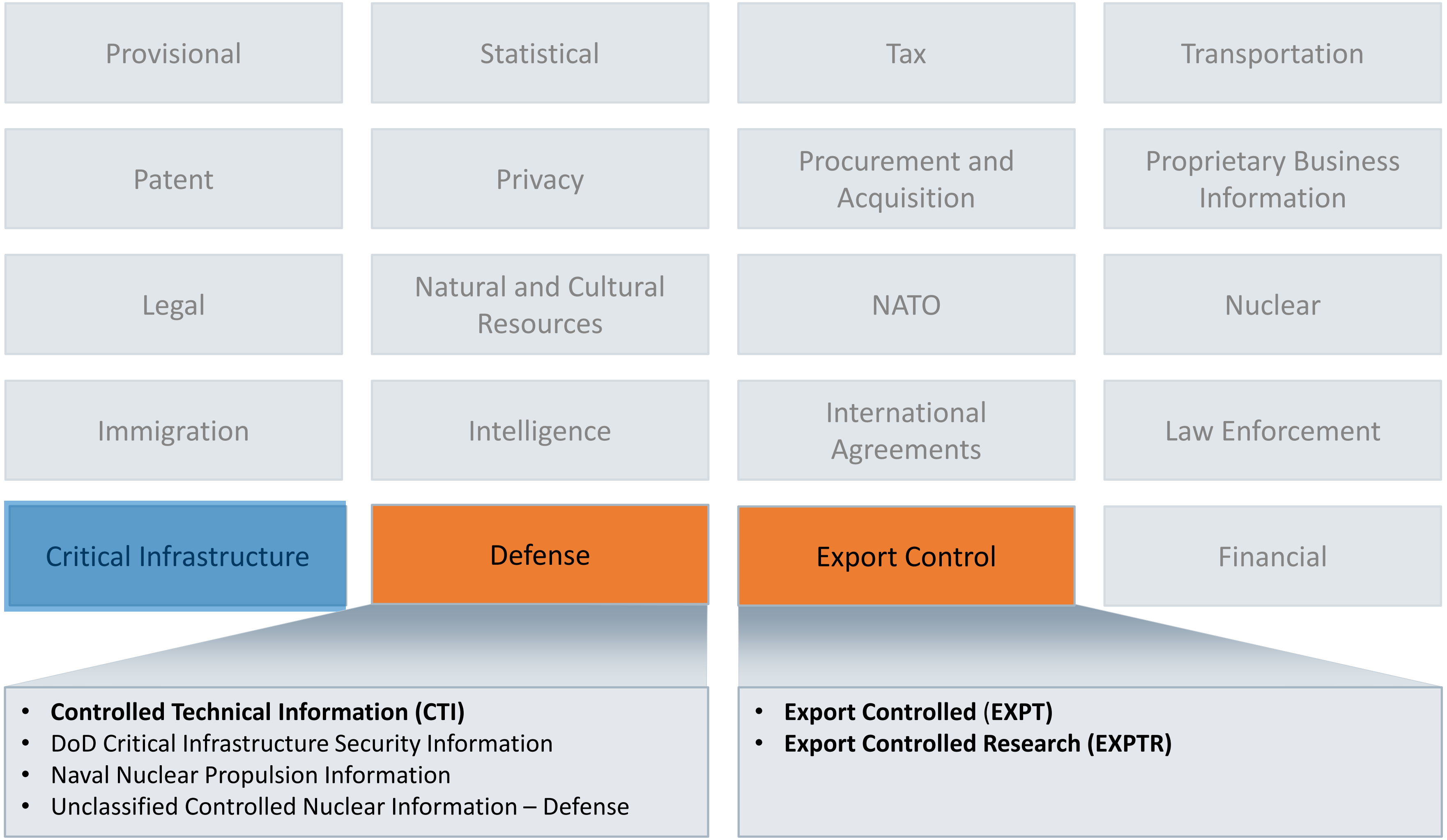
National Archives and Records Administration (NARA)

- Policy, program guidance from the National Security Council
- Serves as the authority on protection of CUI

Information Security Oversight Office (ISOO)

- Contained within NARA
- Responsible to the President for policy and oversight of:
  - The U.S. government’s security classification system

The NARA CUI Registry Categories



Provisional

Statistical

Tax

Transportation

Patent

Privacy

Procurement and Acquisition

Proprietary Business Information

Legal

Natural and Cultural Resources

NATO

Nuclear

Immigration

Intelligence

International Agreements

Law Enforcement

Critical Infrastructure

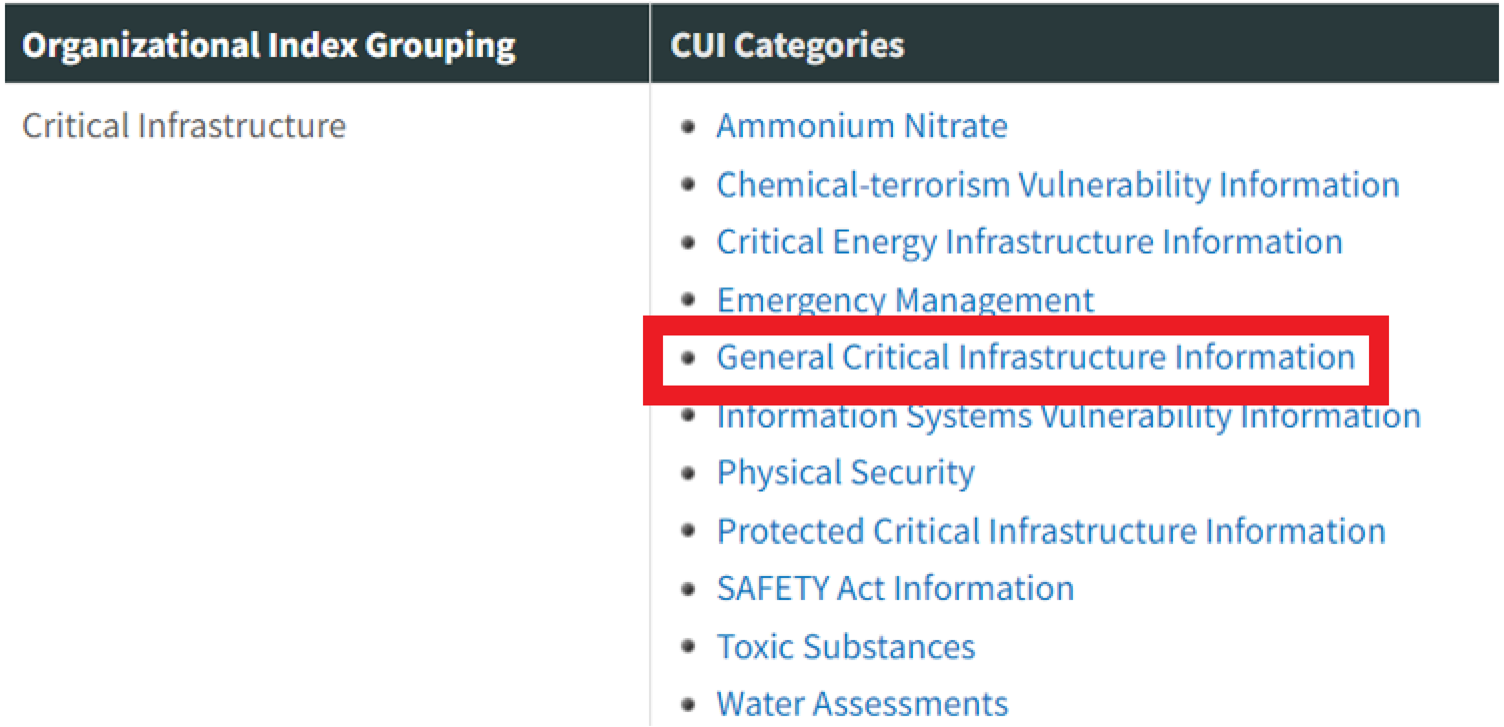
Defense

Export Control

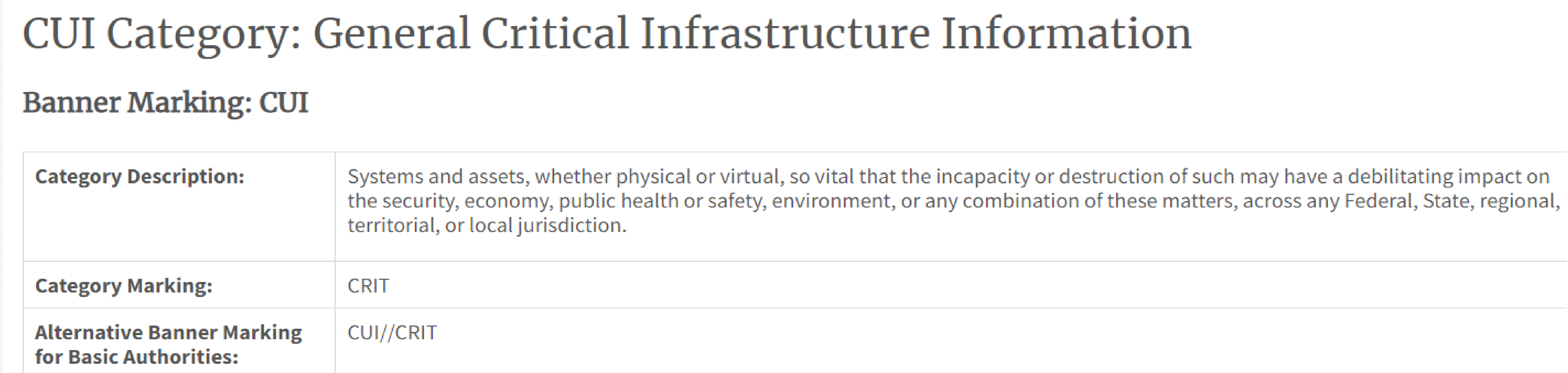
Financial

- **Controlled Technical Information (CTI)**
- DoD Critical Infrastructure Security Information
- Naval Nuclear Propulsion Information
- Unclassified Controlled Nuclear Information – Defense

- **Export Controlled (EXPT)**
- **Export Controlled Research (EXPTR)**



Organizational Index Grouping	CUI Categories
Critical Infrastructure	• Ammonium Nitrate • Chemical-terrorism Vulnerability Information • Critical Energy Infrastructure Information • Emergency Management • General Critical Infrastructure Information • Information Systems Vulnerability Information • Physical Security • Protected Critical Infrastructure Information • SAFETY Act Information • Toxic Substances • Water Assessments



CUI Category: General Critical Infrastructure Information

Banner Marking: CUI

Category Description:	Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any Federal, State, regional, territorial, or local jurisdiction.
Category Marking:	CRIT
Alternative Banner Marking for Basic Authorities:	CUI//CRIT

CMMC requirements based on Sensitivity of Data

Federal Contract Information (FCI) – Level 1

Commercial Companies are holding themselves accountable Federal Contract Information (FCI)

FCI: Information, not intended for public release, that is provided by or generated for the Government under a contract 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 necessary to process payments.

Source: CMMC Glossary and Acronyms (48 CFR 52.204-21)

- FCI is the broadest definition of government information requiring protection
- Characteristics include: Private information and contract related information

  Examples

  - Plans
  - Delivery Dates
  - Schedules
  - Exemptions include:
    - Provided by government or information available on public websites
    - Transactional information. COTS products

CMMC requirements based on Sensitivity of Data

Controlled Unclassified Information (CUI)- Level 2

CUI: Information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and government-wide policies, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.

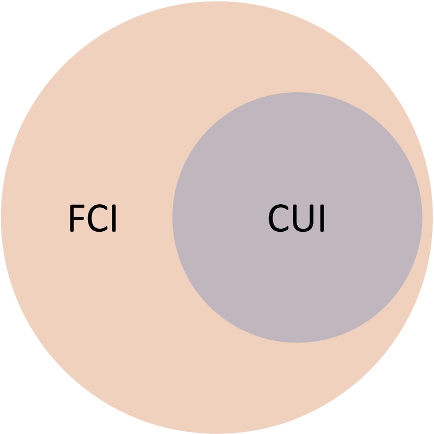
Source: CMMC Glossary and Acronyms (E.O. 13556 (adapted))

- CUI is:
  - Always considered FCI (but not all FCI is necessarily CUI).
  - Not classified information

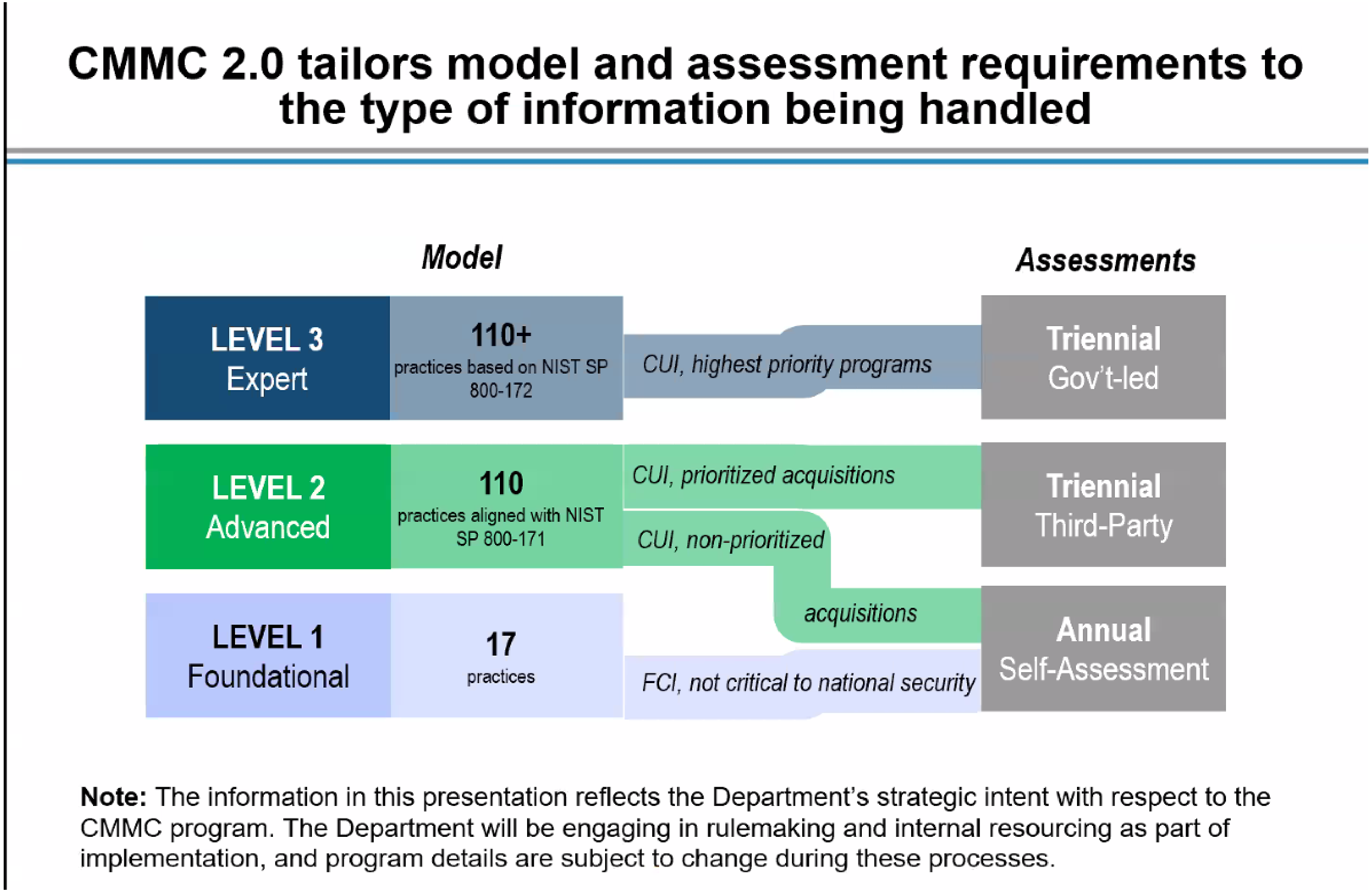
    Information that:
    - The government creates or possesses.
    - An entity creates or possesses on behalf of the government.
    - Requires safeguarding.

Examples:

- Blueprints
- Health information
- Personnel records
- Base civil engineering maps
- Assessment Results/Data



CMMC Levels



CMMC 2.0 tailors model and assessment requirements to the type of information being handled

Model

Assessments

LEVEL 3 Expert — **110+** practices based on NIST SP 800-172 — *CUI, highest priority programs* — **Triennial** Gov't-led

LEVEL 2 Advanced — **110** practices aligned with NIST SP 800-171 — *CUI, prioritized acquisitions* — **Triennial** Third-Party

CUI, non-prioritized acquisitions — **Annual** Self-Assessment

LEVEL 1 Foundational — **17** practices — *FCI, not critical to national security* — **Annual** Self-Assessment

Note: The information in this presentation reflects the Department's strategic intent with respect to the CMMC program. The Department will be engaging in rulemaking and internal resourcing as part of implementation, and program details are subject to change during these processes.

Path to CMMC Level 1 Attestation

1. Understand the CMMC requirements.
   DoD CMMC Model site: https://www.acq.osd.mil/cmmc/model.html
2. Identify the scope (Organizational Unit, Host Unit, Support Units).
3. Conduct a gap analysis.
4. Close any identified gaps.
5. Conduct a self-assessment on an annual basis.
6. Provide a senior official's signature meeting CMMC requirements.
7. Register self-assessments and attestations in the Supplier Performance Risk System (SPRS).

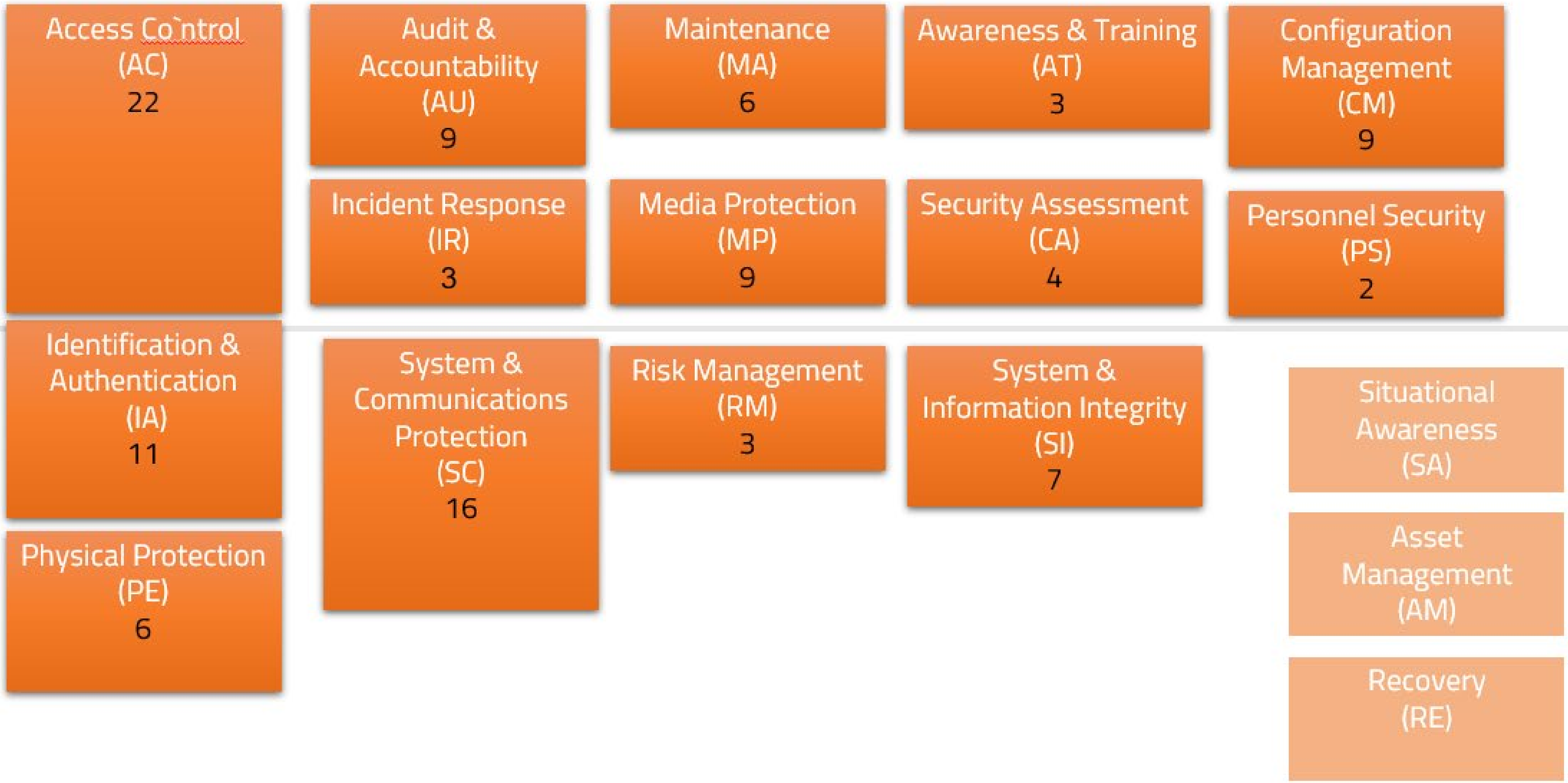
OSC expected to maintain compliance with the CMMC Model during the (1) year.

Path to CMMC Level 2 Certification

1. Understand the CMMC requirements.
   DoD CMMC Model site : https://www.acq.osd.mil/cmmc/model.html
2. Identify the scope (Organizational Unit, Host Unit, Support Units).
3. Conduct a gap analysis.
4. Close any identified gaps.
5. Find C3PAO in the CMMC Marketplace to perform a Level 2 assessment.
6. Assessment is conducted by the C3PAO's certified Assessment Team.
7. C3PAO submits Assessment Report to the DoD.
8. When approved, CMMC Certification is valid for 3 years.

OSC expected to maintain compliance with the CMMC Model during the (3) years.

CMMC DOMAINS → Protect FCI and CUI.



Access Co`ntrol
(AC)
22

Audit &
Accountability
(AU)
9

Maintenance
(MA)
6

Awareness & Training
(AT)
3

Configuration
Management
(CM)
9

Incident Response
(IR)
3

Media Protection
(MP)
9

Security Assessment
(CA)
4

Personnel Security
(PS)
2

Identification &
Authentication
(IA)
11

System &
Communications
Protection
(SC)
16

Risk Management
(RM)
3

System &
Information Integrity
(SI)
7

Situational
Awareness
(SA)

Physical Protection
(PE)
6

Asset
Management
(AM)

Recovery
(RE)

(L) 2002 **Federal Information Security Management Act** (**FISMA**), amended in 2014 as Federal Information Security Modernization Act

- Requires the government to protect sensitive information (such as FCI)

(L) **Executive Order 13556**, Controlled Unclassified Information

- Standardized handling of protected information that is not classified
- CUI is subject to laws governing FCI as well as those specifically for CUI

32 CFR part 2002

- Explains how to comply with EO 13556
- Creates overall requirements, governance, and management if CUI
- NARA to oversee CUI policy, created Information Security Oversight Office which publishes CUI notices

(R) **48 CFR § 52.204-21** – Basic Safeguarding of Covered Contractor Information Systems

- Explain how contractors can adhere to the law
  - Responsibilities when delegating work to a subcontractor (flow down)
  - Requirements and procedure contractors must follow to protect FCI, which include the 17 basic security controls

NIST SP 800-53

- Catalog of security controls for federal information systems
- Defines the cybersecurity requirements for FISMA

NIST SP 800-171

- Catalog of security controls for protection of CUI in non-federal systems
- Based on NIST SP 800-53
- Created by NIST, NARA, in response to EO 13556 and 32 CFR
- Focuses on Confidentiality, does not emphasize integrity of availability

NIST SP 800-171A

- Guide for assessing the security controls defined in NIST SP 800-171

NIST SP 800-172

- A supplement for NIST SP 800-171
- Provides enhanced security requirements
- Adds controls to protect availability and integrity in addition to confidentiality

NIST
National Institute of
Standards and Technology

Department of Commerce is its parent Agency

Numerous publications covering policies

NIST.gov provides publications and resources

Consequence of not meeting CMMC

Failure to receive an award.

- Loss of existing contract.
- Loss of ability to compete on future DoD contracts.

Contractual liability.

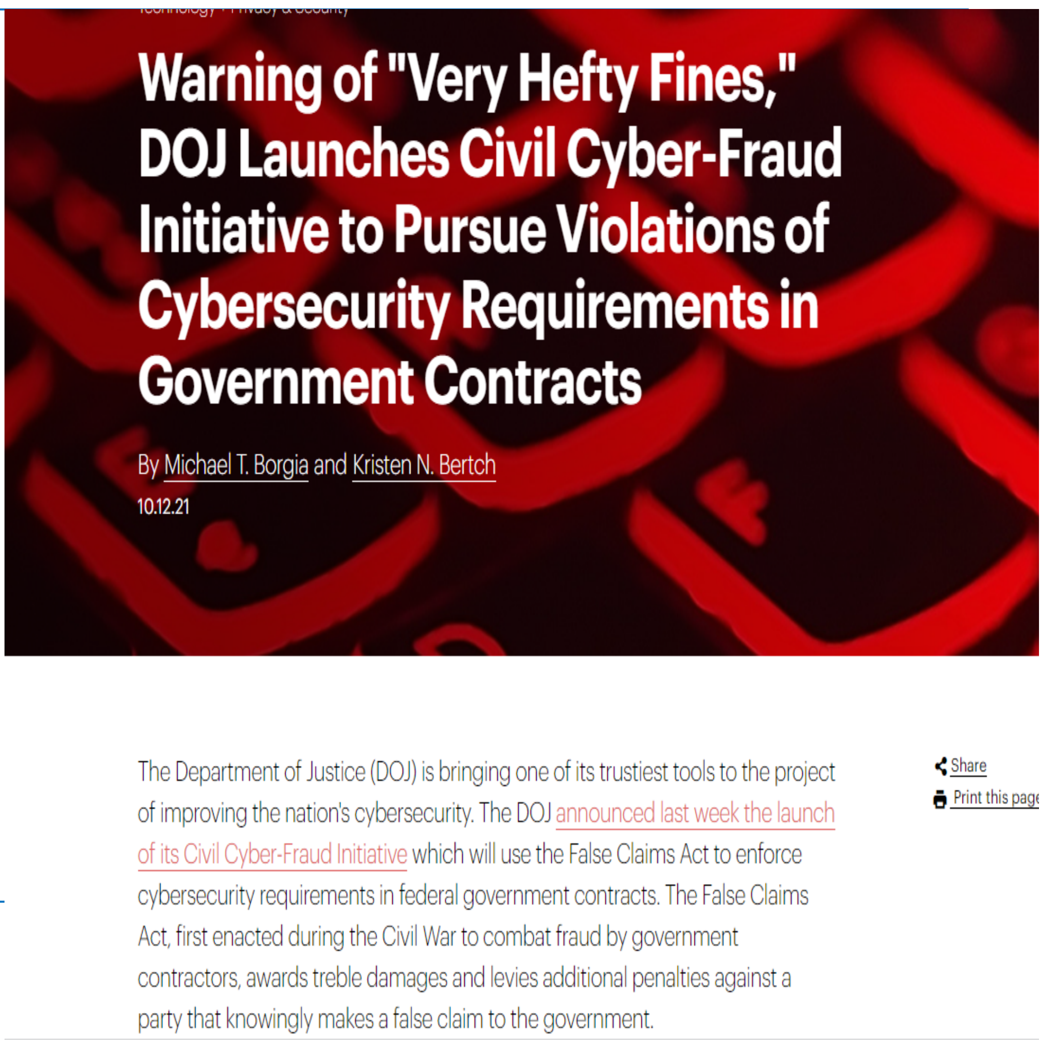
- E.g., breach of contract or civil/criminal penalties.
- Prosecution under the False Claims Act.

Christian Doctrine

- Mandatory procurement statutes/regulations shall be read into federal contracts.
- By operation of law, even if not explicitly stated.

Rationale

Procurement policies set by higher authority cannot be avoided or evaded (deliberately or negligently) by lower government officials.



Technology + Privacy & Security

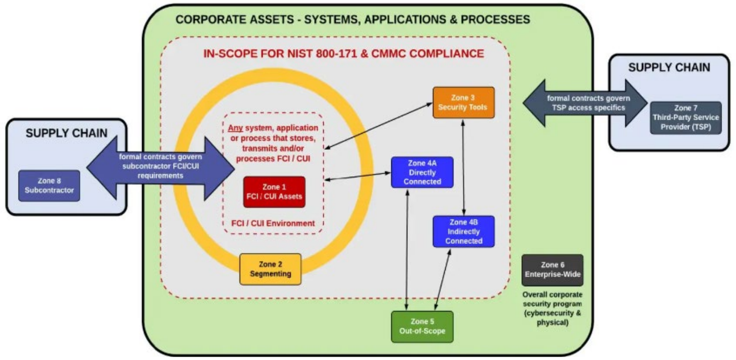
Warning of "Very Hefty Fines," DOJ Launches Civil Cyber-Fraud Initiative to Pursue Violations of Cybersecurity Requirements in Government Contracts

By Michael T. Borgia and Kristen N. Bertch

10.12.21

The Department of Justice (DOJ) is bringing one of its trustiest tools to the project of improving the nation's cybersecurity. The DOJ announced last week the launch of its Civil Cyber-Fraud Initiative which will use the False Claims Act to enforce cybersecurity requirements in federal government contracts. The False Claims Act, first enacted during the Civil War to combat fraud by government contractors, awards treble damages and levies additional penalties against a party that knowingly makes a false claim to the government.

IT Security requires you to know your Information flows


CORPORATE ASSETS - SYSTEMS, APPLICATIONS & PROCESSES
IN-SCOPE FOR NIST 800-171 & CMMC COMPLIANCE
Any system, application or process that stores, transmits and/or processes FCI / CUI
Zone 1 FCI / CUI Assets
FCI / CUI Environment
Zone 2 Segmenting
Zone 3 Security Tools
Zone 4A Directly Connected
Zone 4B Indirectly Connected
Zone 5 Out-of-Scope
Zone 6 Enterprise-Wide
Overall corporate security program (cybersecurity & physical)
SUPPLY CHAIN
formal contracts govern TSP access specifics
Zone 7 Third-Party Service Provider (TSP)
SUPPLY CHAIN
formal contracts govern subcontractor FCI/CUI requirements
Zone 8 Subcontractor

CYBERSECURITY MATURITY MODEL CERTIFICATION CENTER OF EXCELLENCE

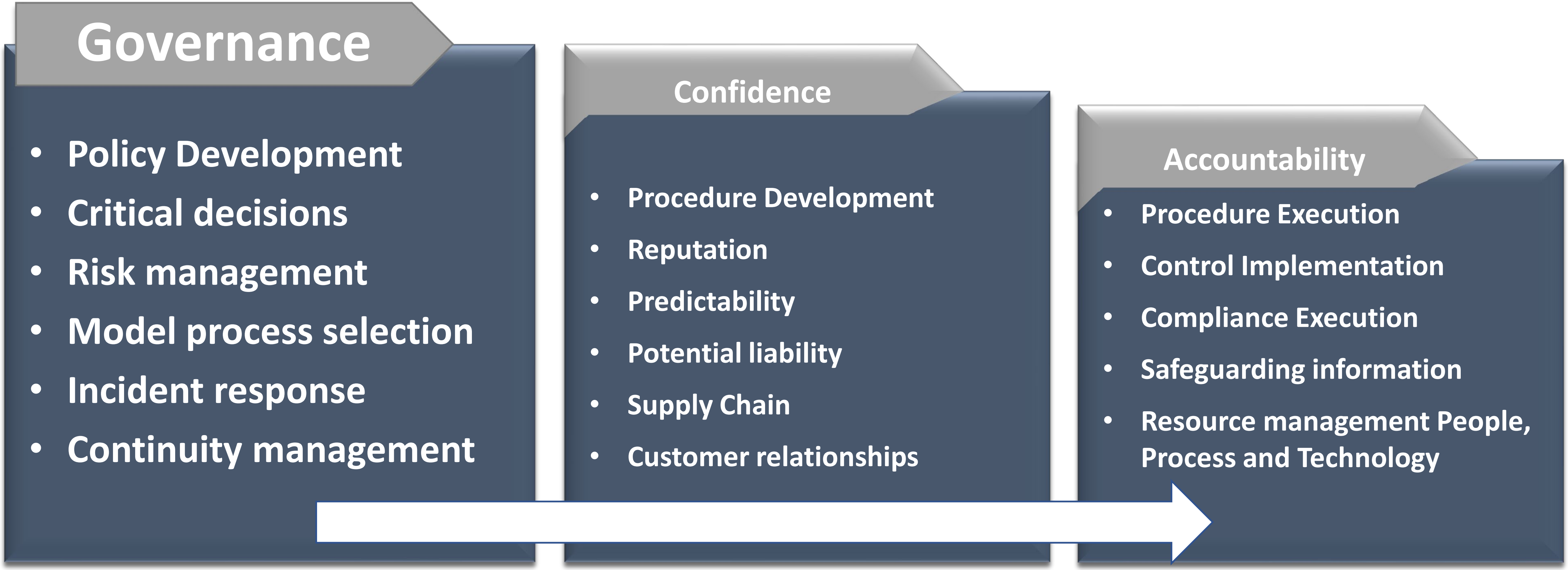
NIST National Institute of Standards and Technology

Understand how your Information flows

Use a Maturity Model to protect your Information flows

All Cyber Maturity Models lead to NIST

Development of your Cyber Program



Governance

- Policy Development
- Critical decisions
- Risk management
- Model process selection
- Incident response
- Continuity management

Confidence

- Procedure Development
- Reputation
- Predictability
- Potential liability
- Supply Chain
- Customer relationships

Accountability

- Procedure Execution
- Control Implementation
- Compliance Execution
- Safeguarding information
- Resource management People, Process and Technology

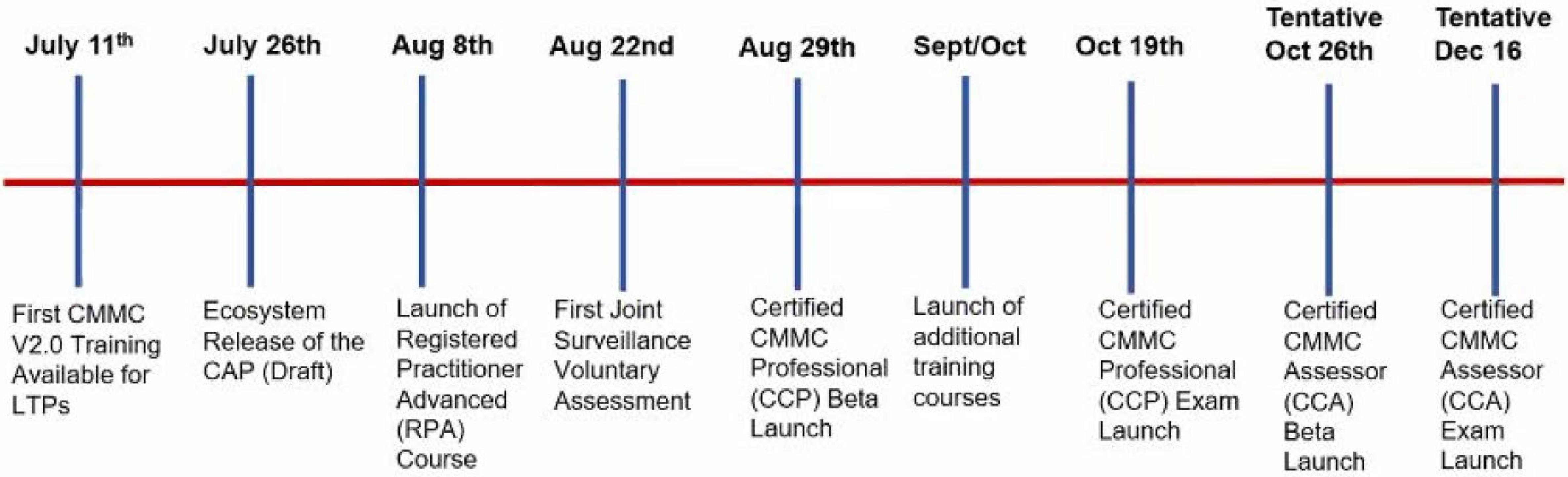
2022 H2 Momentum

Gradual role out to CMMC

CMMC December 2021 Model 2.0 released

May 2023 CMMC Expected Rule Making add to the DFARs

December 2025 all contracts required CMMC



July 11th
First CMMC V2.0 Training Available for LTPs

July 26th
Ecosystem Release of the CAP (Draft)

Aug 8th
Launch of Registered Practitioner Advanced (RPA) Course

Aug 22nd
First Joint Surveillance Voluntary Assessment

Aug 29th
Certified CMMC Professional (CCP) Beta Launch

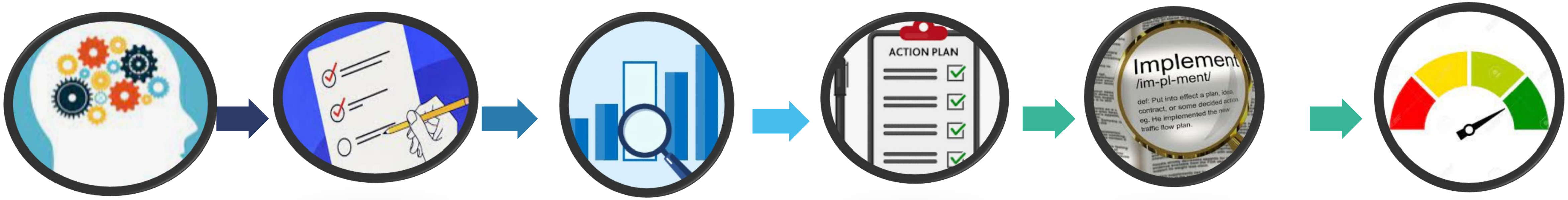
Sept/Oct
Launch of additional training courses

Oct 19th
Certified CMMC Professional (CCP) Exam Launch

Tentative Oct 26th
Certified CMMC Assessor (CCA) Beta Launch

Tentative Dec 16
Certified CMMC Assessor (CCA) Exam Launch

Cyber Assessment Life-Cycle Flow


ACTION PLAN
Implement
/im-pl-ment/
def: Put into effect a plan, idea, contract, or some decided action
eg. He implemented the new traffic flow plan.

Step 1:
Learn how Cyber Assessment models will benefit the organization

Step 2:
Establish cyber improvement objectives aligned to your organizational objectives

Step 3:
Map current organizational processes to Cyber model practices

- People
- Process
- Technology

Step 4:
Develop and follow action plans and keep updated

Step 5:
Deploy Cyber improvements and measure results

Step 6:
Evaluate capability and assess Cyber performance

TIME needed for Cyber Assessment

EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Pacific Northwest
NATIONAL LABORATORY

American Water Works Association

Dedicated to the World's Most Important Resource®

PROTECTING AMERICAN ASSETS

DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA

North American Transmission
FORUM

U.S. DEPARTMENT OF
ENERGY

Questions?

Dean Rock, SteelToad
dean.rock@steeltoad.com
240.988.1876