



# Pub K

**PUBLIC CONTRACTS**

**Annual Review 2022**

**January 24 – 27, 2022**

## DAY 2

12:00 p.m. Costs, Pricing & Audits

2:00 p.m. Grants & Cooperative Agreements

3:00 p.m. Cybersecurity & IT

TUESDAY, JANUARY 25, 2022

12:00 PM to 5:00 PM

Pub K

PUBLIC CONTRACTS



Alan Chvotkin  
President, Pub K  
Partner, Nichols Liu LLP

## News for the Government Contracts Community

Pub K

PUBLIC CONTRACTS | LAW

Legal decisions and developments for the government contracts community

Pub K

PUBLIC CONTRACTS | CYBER

Monitoring the government response to cybersecurity threats and trends

Pub K

PUBLIC CONTRACTS | COMPLIANCE

Developments and insights in ethics, compliance, and FCA/FCPA enforcement

For more information  
Visit <https://pubkgroup.com/features/>

Pub K

PUBLIC CONTRACTS

Event Sponsors

Platinum Sponsor

NICHOLS LIU

SERVING GOVERNMENT CONTRACTORS

Gold Sponsors

pillsbury

VENABLE LLP

Silver Sponsors

Arnold & Porter

MORRISON  
FOERSTER

COVINGTON

HK>A

Vinson & Elkins

wiley

BLANKROME  
CELEBRATING 75 YEARS

PILIERO  
MAZZA

DLA PIPER

crowell|moring

bakertilly

Holland & Knight

SheppardMullin

PERKINS coie  
COUNSEL TO GREAT COMPANIES

BRG  
Berkeley Research Group

GT GreenbergTraurig

JENNER & BLOCK

# Today's Event Supports





## Tips for a Good Viewing Experience

This webinar is being streamed live and is presented in listen-only mode. Your video will remain disabled throughout the session.

For the best audio quality, please ensure your computer speakers are turned on and the volume is up.

We recommend closing any programs or browser sessions that could disrupt your connection.

You might try using Chrome for a more stable experience or refresh the webpage.

## Audience Notes

- Q&A – to ask a question of the panel, please type your comment in the Q&A box at the bottom of your screen. The panel will address as many questions as time allows.
- Materials
  - Available for download at <https://pubkgroup.com/pubk-annual-review-2022/>

## CLEs

Pub K is applying for CLE approval for the Annual Review in Virginia, California, Texas, Florida, Colorado, and Kansas.

- Approval is expected but not guaranteed
- Pub K will notify participants of approval when received
- CLEs are available free of charge to Pub K subscribers
- For non-subscribers, the fee is \$75 for 1 CLE and \$150 for 2 or more
- Email [craig@pubklaw.com](mailto:craig@pubklaw.com) with questions.

## CLEs

**Important:** Many state boards require us to verify participation *during* the event.

Watch for this poll question during the panel:

Thank you for attending today's panel! Please respond to our survey if you are interested in obtaining CLEs for this session.

We will record your response to verify your participation for the CLE certificate.

# Event Sponsors

Platinum Sponsor

**NICHOLS LIU**

SERVING GOVERNMENT CONTRACTORS

Gold Sponsors

**pillsbury**

**VENABLE** LLP

Silver Sponsors

Arnold & Porter

MORRISON  
FOERSTER

COVINGTON

HK>A

Vinson & Elkins

wiley

BLANKROME  
CELEBRATING 75 YEARS

PILIERO  
MAZZA

DLA PIPER

crowell|moring

bakertilly

Holland & Knight

SheppardMullin

PERKINS coie  
COUNSEL TO GREAT COMPANIES

BRG  
Berkeley Research Group

GT GreenbergTraurig

JENNER & BLOCK

## SESSION 6

# CYBERSECURITY AND INFORMATION TECHNOLOGY (CMMC)

TUESDAY, JANUARY 25, 2022

3:00 PM to 4:50 PM

Pub K

PUBLIC CONTRACTS



Townsend L. Bourne, Partner

**SheppardMullin**





Robert S. Metzger, Shareholder



ROGERS | JOSEPH | O'DONNELL



Kate M. Growley, Partner

crowell  moring



Kristin Marie Grimes  
Assistant General Counsel  
National Security & Cyber Law Branch, FBI

# Agenda (Part I)

- I. Setting the Stage
- II. Federal Law Enforcement: the FBI Perspective
- III. Executive Order 14028
- IV. Ransomware
- V. Supply Chain Risk Management
- Break for Q&A

# Agenda (Part 2)

- VI. Cyber Regulation and CMMC
- VII. DOJ Civil Cyber Fraud Initiative
- VIII. Other Issues
  - ▷ Privacy & Security
  - ▷ Cyber OT
  - ▷ IoT Risk & Regulation
- Final Q&A

# I. Setting the Stage: 2021 Cyber SCRM Year in Review

2021 was a grim year for cyber / SCRM

- ▷ SolarWinds (initially detected [Dec. 2020](#))
- ▷ [Emergency Directive](#): Microsoft Exchange Server (Hafnium) (Jan. 2021)
- ▷ Colonial Pipeline ransomware attack (May 2021)
- ▷ JBS ransomware attack (May 2021)
- ▷ Kaseya supply chain ransomware attack (Jul. 2021)
- ▷ Apache Log4j Open Source SW [Emergency Directive](#) (Dec. 2021)
- ▷ [Microsoft](#): “Destructive malware targeting Ukrainian organizations (Jan. 2021)

Ukraine: now



# Multiple Attack Vectors



## CYBER-IT

**EXFILTRATION**

**EXTORTION**

**DENIAL**

**CORRUPTION**

**DESTRUCTION**

## CYBER/PHYSICAL- OT



Natanz, Iran



Bowman Dam, NY

## Supply Chain



SOFTWARE  
HARDWARE  
FIRMWARE  
SERVICE PROVIDERS  
THE WORKFORCE

### **“Researchers Discover Dangerous Firmware- Level Rootkit”**

*DARKReading*  
Jan. 20, 2021

“Morgan Stanley has  
joined the growing list  
of [Accellion](#) hack victims  
— more than six months  
after attackers first  
breached the vendor’s 20-  
year-old file-sharing  
product.

*TechCrunch*  
July 8, 2021

**“The ‘human factor’ has been recognized as the weakest  
link in creating safe and secure digital environments ”**

Source: [Security Magazine](#)

**“Our supply chains are exposed to  
multiple threat vectors.** Supply chains  
are one of the four primary elements  
of an adversarial attack via blended  
operations. Attacks may be mounted  
**against the entire supply chain life  
cycle** from conception to retirement.  
The supply chain is vulnerable to  
adversary insertion of counterfeit  
parts that pass ordinary inspection  
but fail operationally. Largely through  
cyber-physical threats, **adversaries  
may introduce malware or exploit  
latent vulnerabilities in firmware or  
software** to produce adverse,  
unintended, and unexpected physical  
effects on connected or controlled  
systems. **Supply chains as a service  
present another critical exploitation  
vector.”**

MITRE Deliver Uncompromised [Report](#), at 7.

# CMMC: from 1.0 to 2.0 ( ... pending rulemaking)

<p>Draft – Pre-decisional</p> <p><b>DFARS Case 2019-D041</b></p> <p><b>Assessing Contractor Implementation of Cybersecurity Requirements</b></p>		
<p>The <i>interim rule</i> took effect 30 Nov 2020 / DoD implementing a 5-year phased roll-out</p>		
<p><b>DFARS Provision 252.204-7019</b> Notice of NIST SP 800-171 DoD Assessment Requirements</p> <p><b>Solicitation Notice: Basic Assessment Score required in SPRS for contract award</b></p> <ul style="list-style-type: none"> <li>A <a href="#">NIST SP 800-171 DoD Assessment</a> (Basic, Medium, High) summary level score must be posted into DoD's Suppliers Risk Performance System (SPRS) for the applicable CAGE code and Systems Security Plan</li> <li>The summary level score must remain current (not older than 3 years unless a lesser time is specified) throughout the life of the contract, task or delivery order</li> </ul>	<p><b>DFARS Clause 252.204-7020</b> NIST SP 800-171 DoD Assessment Requirements</p> <p><b>Basic Assessment Score required in SPRS to be considered for contract award</b></p> <ul style="list-style-type: none"> <li>Applicable to companies subject to DFARS clause 252.204-7012</li> <li>Post award, if DoD deems a Medium or High assessment is necessary due to program sensitivity, provide DoD access to facilities, systems and personnel</li> <li>Include clause in all subcontracts or other contractual instruments including subcontracts for commercial items</li> <li>Confirm subcontractor compliance with SPRS reporting if receiving CUI</li> </ul>	<p><b>DFARS Clause 252.204-7021</b> Cybersecurity Maturity Model Certification Requirements</p> <p><b>Cybersecurity Maturity Model Certification Required by contract award effective 1 Oct 2025</b></p> <ul style="list-style-type: none"> <li>Until 1 Oct 2025, OUSD(A&amp;S) must approve clause in new acquisitions</li> <li>Contractor certification level must be maintained for contract duration</li> <li>Clause must be flowed down; primes must ensure subs are certified at required CMMC level prior to awarding subcontract</li> </ul> <p><b>Interim rule clauses are applicable to contracts, task orders and delivery orders</b></p> <p><b>Not applicable to micro-purchases or solicitations exclusively for the purchase of COTS products</b></p>
<p><b>CMMC assessments and certifications required for the applicable enterprise network or network segment where FCI or CUI will be processed, stored, or transmitted in performance of the contract</b></p>		

CMMC 1.0 sought too much, of too many, and too fast. It has been replaced with CMMC 2.0, which requires new rulemaking over 12-24 months. In the interim, FAR and DFARS clauses remain in effect to protect “Federal Contract Information” (FCI) and “Controlled Unclassified Information” (CUI).

The CMMC experience so far does not promote confidence that cyber and supply chain security can be accomplished through regulations, contract terms and mandatory third-party assessments. But the prior approach of relying upon “self attestation” did not succeed and federal contractors, civil or DoD, are now subject to more threat actors, more threat types, greater risks and rising impacts to the contractor enterprise as well as government customers. Improved security is an imperative: but how?



## II. FBI Cyber Mission Statement

The purpose of FBI Cyber is to **impose risk and consequence** on cyber adversaries to ensure the United States' safety, security, and confidence in a digitally-connected world.

The FBI uses its **unique authorities, world-class capabilities, and enduring partnerships** to complete an essential mission for the U.S. Government's effort to shape an ever-changing and increasingly complex cyber ecosystem.

## Imposing Risk & Consequence on Adversaries



Unveil



Seize



Shut



Takedown



Unlock

# Cyber Crime Trends



Business Email  
Compromise



Tech Support

192.168.3.2.1

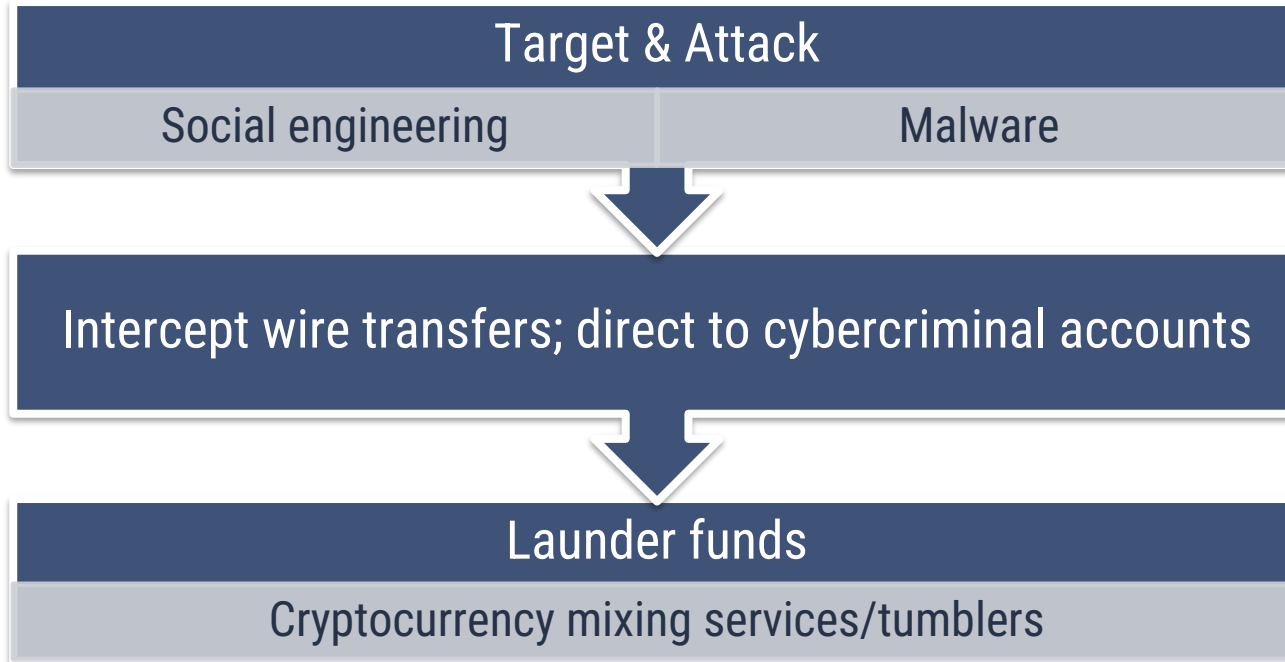


Ransomware

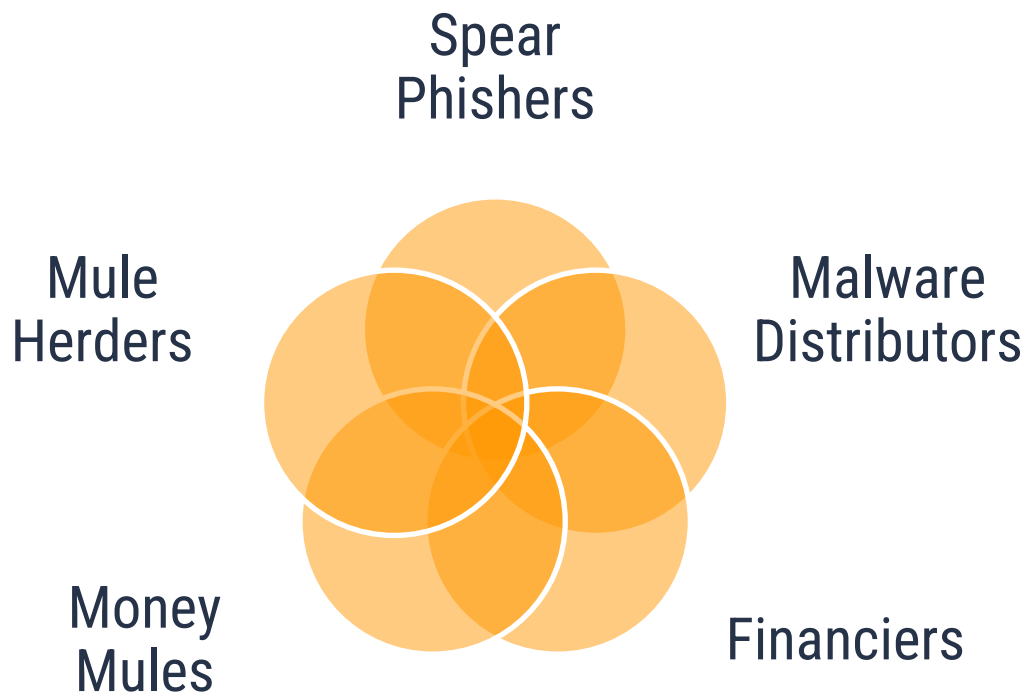


Elder Fraud

# Business Email Compromise



# Business Email Compromise: Roles in the BEC Network



# Business Email Compromise: Response & Protection

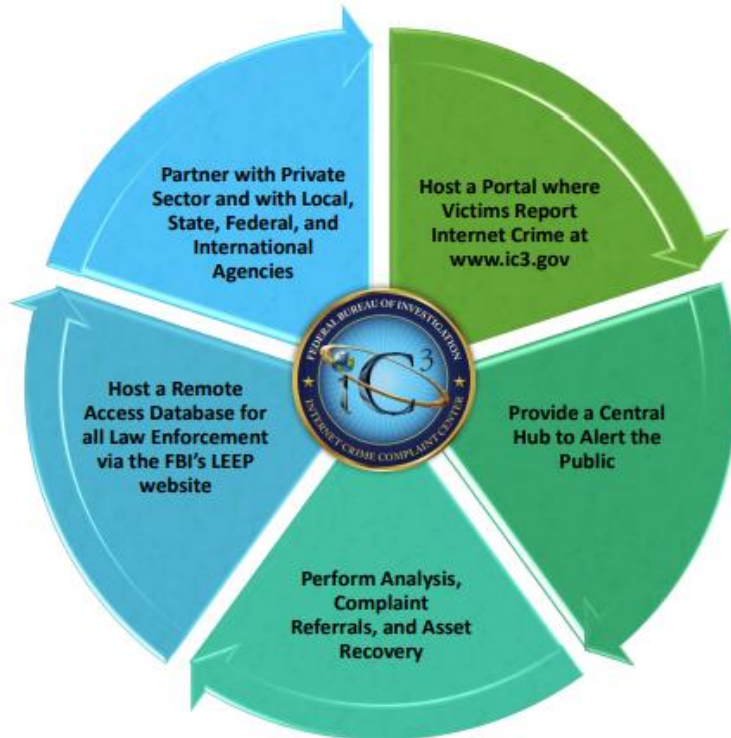
## Defend

- Proper training
- Verify payment changes
- Hover over/expand contact details on suspicious email addresses
- Technical tools
  - intrusion detection systems
  - email authentication protocol

## Respond

- Contact the originating financial institution
  - Request wire recall or reversal
- File a detailed complaint with [www.ic3.gov](http://www.ic3.gov)
  - Include detailed account information
  - Leverage Recovery Asset Team

# Report Cyber Intrusions to IC3.gov

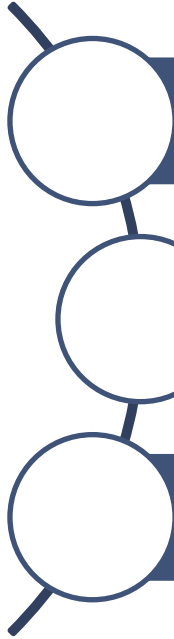


## Recovery Asset Team (RAT):

Created to streamline communication with financial institutions and assist with the recovery of funds for victim companies who made transfers to domestic accounts under fraudulent pretenses.

In 2020 alone, RAT stopped over \$380 million from being stolen from individuals and businesses

## Engaging with You



Develop a relationship with the FBI and with your local FBI field office

Develop a formal incident response plan and include your local FBI field office in that plan

In the event of an intrusion, make sure you report the compromise early to your local FBI field office or to [ic3.gov](https://ic3.gov)



If you remember one thing...



## It's about time

- Engage with us early
- Report intrusions quickly
- It's never too late to reach out

***Add to our joint story of successful defense, response,  
and recovery***

# Executive Order 14028: Improving Cybersecurity (May 2021)

- Sharing Threat Information (Sec. 2)
- Modernizing Federal Government Cybersecurity (Sec. 3)
- Enhancing Software Supply Chain Security (Sec. 4)
- Cyber Safety Review Board (Sec. 5)
- Government Playbook to Respond to Cyber Vulnerabilities and Threats (Sec. 6)
- Steps for the Government to Maximize Early Detection of Vulnerabilities & Incidents (Sec. 7)
- Government improvement of its Cyber Investigation and Remediation Capabilities (Sec. 8)
- Updates to Requirements for the National Security Systems (Sec. 9)

## **Executive Order 14028: Improving Cybersecurity (May 2021); Sharing Threat Information (Sec. 2)**

- Remove contractual barriers to IT, OT, and cloud service providers sharing cyber threat and incident information
- ICT service providers must promptly report cyber incidents
- Streamline/standardize cybersecurity contractual requirements across agencies

## Executive Order 14028: Improving Cybersecurity (May 2021); Sharing Threat Information (Sec. 2)

### ■ Open FAR Cases:

- ▶ 2021-019 – Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems
- ▶ 2021-017 – Cyber Threat and Incident Reporting and Information Sharing (Consolidates IT/OT and ICT service provider reporting provisions)

■ Draft proposed rules in process; due Feb. 2, 2022

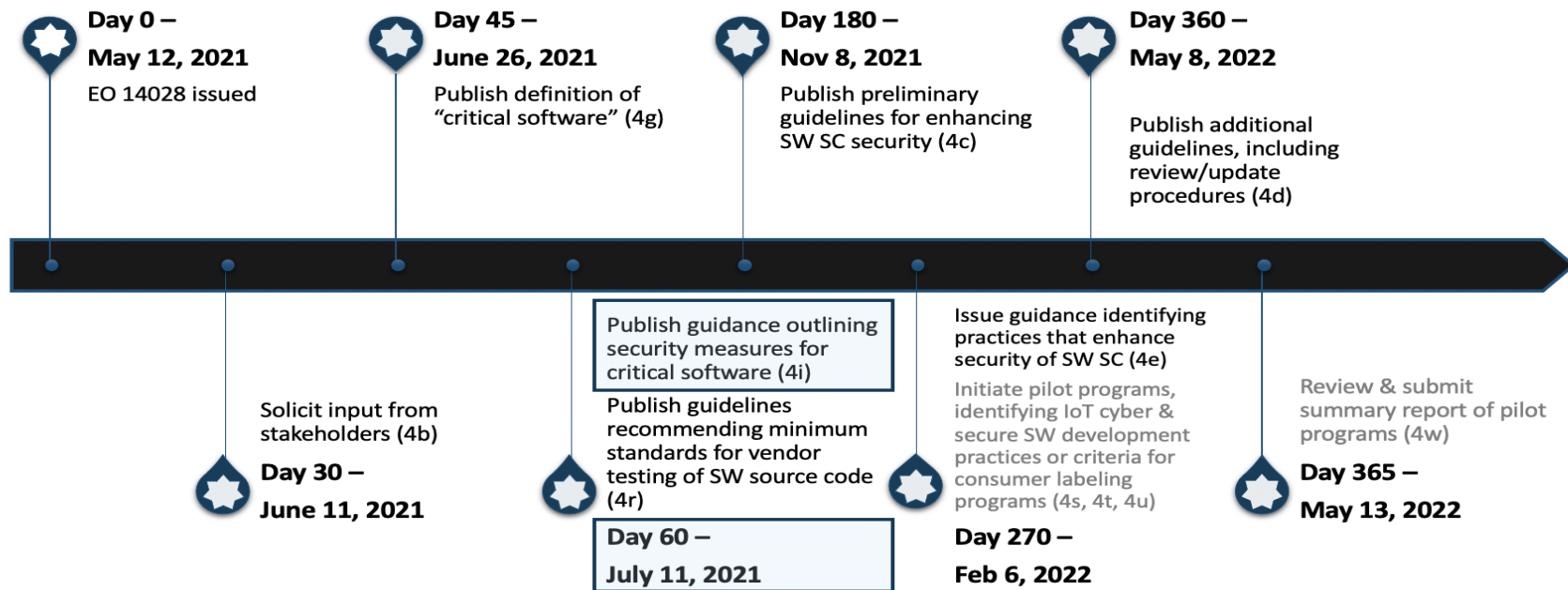
## Executive Order 14028: Improving Cybersecurity (May 2021); Modernizing Federal Cyber (Sec. 3)

- Requires the government to modernize its approach to cybersecurity
  - ▷ Prioritize cloud solutions
  - ▷ Move towards Zero Trust Architecture
  - ▷ Adopt MFA and encryption
  - ▷ Modernize FedRAMP

## **Executive Order 14028: Improving Cybersecurity (May 2021); Software Supply Chain Security (Sec. 4)**

- NIST definition of “critical software”
- Preliminary and updated guidance from NIST on enhancing software supply chain security
- Minimum elements for an SBOM
- FAR updates – software providers to attest to compliance with new requirements (May '22)
- Development of criteria for consumer labeling program for software and IoT

# NIST EO Section 4 Timeline



<https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/software-supply-chain-security>

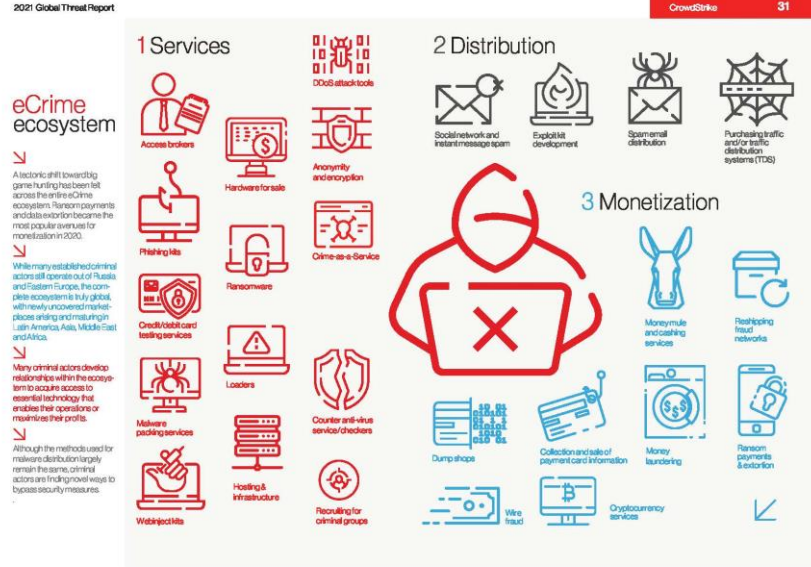
# Ransomware

## Three Tiers of Ransomware Threats

Tactic	Extortion	Demand
Encrypt	Single	Request payment for the encryption key
	Double	Threaten public exposure of the data
Exfiltrate		Threaten end customers / patients to avoid public exposure of the data
DDoS	Triple	Threaten a DDoS attack to bring the victim back to the negotiation table

Source: BitSight, [Ransomware: The Rapidly Evolving Threat](#)

## Now a massive, global criminal enterprise



Source: CrowdStrike, [2021 Global Threat Report](#)

And: nation states accommodate, facilitate, host, promote, coopt or use ransomware



# Ransomware Threats & Gov Contractors

- Ransomware greatly aggravates the risk of porous enterprise security – for all enterprises (in the DIB or not).
- DIB measures (7012) focus on information “confidentiality” but not “integrity” or availability.”
- Nation state actors were the threat driver for CMMC. Criminal enterprises are the prime ransomware actors, but nation state use is present too.
- Attackers now use the “double extortion” technique which both denies access to enterprise records *and* exfiltrates those records with threat of disclosure to the public or to business rivals. Triple extortion can shut the info system of the target enterprise.
- Where personal information is among the records so stolen, the release could trigger many forms of exposure under laws and regs that protect privacy.

# Ransomware: Enterprise Damage & Liability Risk

## Among the many business risks and adverse legal consequences to a ransomware attack:

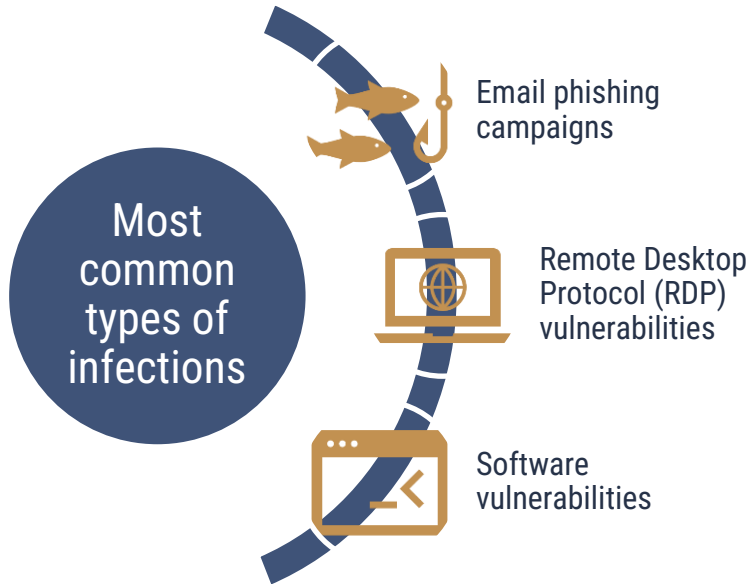
- Business interruption loss, to the extent not covered by insurance;
- Direct costs – immediate response costs (attorneys, forensic specialists, etc.), costs of ransom paid, cost of restoration and recovery, breach notification and remedial measures;
- Regulatory actions (including fines) from Treasury, SEC, FTC and other federal agencies;
- Liability exposure to persons whose privacy interests are injured; potential financial penalties imposed by EU Data Protection Authorities (DPAs) under the GDPR (or CCPA);
- Defense of 3d party legal actions from customers or supply chain partners whose confidential information is compromised, or for breach of contract where performance impaired or delayed;
- Liability claims from affected or injured shareholders, lenders or other investors;
- Insurance coverage disputes, limitation or denial of coverage or increased coverage
- Loss of confidence of business partners and damage to consumer confidence and brand value;
- Potential FCA exposure? E.g., for a wilfull failure to follow required cybersecurity standards, including failure to report a breach, if material to the Government's decision to do business with a supplier.

### THE WHITE HOUSE

#### Fact Sheet: Ongoing Public U.S. Efforts to Counter Ransomware October 13, 2021

The Biden Administration has pursued a focused, integrated effort to counter the threat. Yet, government action alone is not enough. The Administration has called on the private sector, which owns and operates the majority of U.S. critical infrastructure, to modernize their cyber defenses to meet the threat of ransomware. The Administration has announced specific efforts to encourage resilience, including voluntary cyber performance goals, classified threat briefings for critical infrastructure executives and the Industrial Control Systems Cybersecurity Initiative. And, the Administration has stepped up to lead international efforts to fight ransomware. International partnership is key since transnational criminal organizations are often the perpetrators of ransomware crimes, leveraging global infrastructure and money laundering networks to carry out their attacks

# Ransomware



## FBI does not recommend paying ransom

- Doesn't guarantee regaining access to data
- Emboldens adversary
- Can fund illicit activity & potential OFAC sanctions violations

## Supply Chain Risk Management: Section 889

■ “Covered telecommunications equipment or services” includes:

- ▶ Equipment and services from **Huawei Technologies Company** or **ZTE Corporation** (or any subsidiary or affiliate of such entities)
- ▶ In the public safety context, surveillance equipment or services produced by **Hytera Communications Corporation**, **Hangzhou Hikvision Digital Technology Company**, or **Dahua Technology Company** (or any subsidiary or affiliate of those entities)
- ▶ Other entities as determined by the Secretary of Defense

■ Applies to ALL contractors (no COTS, micro-purchase, or small business exclusion)

## Supply Chain Risk Management: Section 889

■ Part A – went into effect August 2019; FAR updated via interim rule (FAR Case 2018-017)

- ▶ Prohibits contractors from selling the Government equipment or services that incorporate Huawei et al. technology (FAR 52.204-25)
- ▶ Requires contractor representation prior to award (FAR 52.204-24)
- ▶ Reporting requirement (within one business day!) for any covered equipment or services discovered during contract performance; mandatory flow-down (FAR 52.204-25)

## Supply Chain Risk Management: Section 889

- Part B – went into effect August 2020; FAR updated via interim rule (FAR Case 2019-009)
  - ▶ Prohibitions on companies that *USE* the covered products or services, even if not part of federal business
  - ▶ Part B representation added to the FAR (limited to offeror entity); reasonable inquiry standard
  - ▶ Reporting requirement applies; Part B need not be flowed-down
- Report for final rules for both FAR Cases currently due this month

## Supply Chain Risk Management: FASC Final Rule

- Required by the Federal Acquisition Supply Chain Security Act of 2018 (FASCSA)
- Interim rule issued September 1, 2020
- Final rule issued August 26, 2021
- Outlines processes and procedures for FASC to evaluate supply chain security risk
- Does not specifically name entities (Sources) or products (Covered Articles) that pose risk

## Supply Chain Risk Management: FASC Final Rule

- DHS responsible for procedures of SCRM Task Force
- Agencies must submit information regarding substantial supply chain risk
  - ▶ Non-federal entities may voluntarily submit information
- Evaluation – rule includes 10 non-exclusive factors
- Recommendation – may be Exclusion or Removal of covered articles or sources from agency procurements
- Compliance – agencies may be granted waivers



## Supply Chain Risk Management: Commerce Interim Rule on ICT Transactions

- Implements EO 13873, Securing ICT Supply Chain from cyberespionage
- Agencies may request Commerce review ICT transactions between U.S. persons and persons subject to foreign adversary for “undue and unacceptable risk”
- May potentially block transaction or propose mitigation measures

## Supply Chain Risk Management: Other Initiatives

- NIST 800-161 Rev. 1 (Draft – Oct. 2021) – guidance on identifying, assessing, and mitigating cyber supply chain risks
- 2019 NDAA, Section 1655 – would require disclosure to DoD in certain circumstances if source code may be reviewed by foreign government or person
  - ▶ DFARS Case 2018-D064 “on hold”
- 2020-2022 NDAA's



# Question Set 1

## Contractor Cyber Regulation: Current State of Play

- FAR 52.204-21, *Basic Safeguarding of Covered Contractor Information Systems*
- DFARS 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*
- DFARS 252.204-7019, *Notice of NIST SP 800-171 DoD Assessment Requirements*
- DFARS 252.204-7020, *NIST SP 800-171 DoD Assessment Requirements*
- DFARS 252.204-7021, *Contractor Compliance with the Cybersecurity Maturity Model Certification (CMMC) Level Requirements*

## Cybersecurity Maturity Model Certification (CMMC)

- March 2021: DoD begins internal assessment of CMMC
- Nov. 2021: DoD announced “CMMC 2.0” with multiple changes intended to streamline requirements and process
- Compliance (DFARS 252.204-7021) not required until corresponding rulemaking complete
- Rulemaking anticipated to take 9-24 months

# Cybersecurity Maturity Model Certification (CMMC)

Model		Assessment	CMMC Model 1.0
171 practices	5 processes	Third-party	<b>LEVEL 5</b> Advanced <i>CUI, critical programs</i>
156 practices	4 processes	None	<b>LEVEL 4</b> Proactive <i>Transition Level</i>
130 practices	3 processes	Third-party	<b>LEVEL 3</b> Good <i>CUI</i>
72 practices	2 maturity processes	None	<b>LEVEL 2</b> Intermediate <i>Transition Level</i>
17 practices		Third-party	<b>LEVEL 1</b> Basic <i>FCI only</i>

Source: DoD's Advanced Notice of Proposed Rulemaking Announcing CMMC 2.0, dated 17 November 2021, and DoD's CMMC Version 2.0 Briefing, dated 3 December 2021.

# Cybersecurity Maturity Model Certification (CMMC)

## CMMC Model 2.0

	Model	Assessment
<b>LEVEL 3</b> Expert	<b>110+</b> practices based on NIST SP 800-172	Triennial government-led assessments
<b>LEVEL 2</b> Advanced	<b>110</b> practices aligned with NIST SP 800-171	Triennial third-party assessments for critical national security information; Annual self-assessment for select programs
<b>LEVEL 1</b> Foundational	<b>17</b> practices	Annual self-assessment

Source: DoD's Advanced Notice of Proposed Rulemaking Announcing CMMC 2.0, dated 17 November 2021, and DoD's CMMC Version 2.0 Briefing, dated 3 December 2021.

## Cybersecurity Maturity Model Certification (CMMC)

- ✗ CMMC-specific practices
- ✗ Maturity processes
- ✗ C3PAO assessments for all certifications
- ✓ Plans of action and milestones (POAMs) (with limits)
- ✓ Senior company official attestations
- ✓ Program waivers



# Cybersecurity Maturity Model Certification (CMMC)

- Dec. 2021: Scoping and Assessment Guidance released for Levels 1 & 2
- Introduced new forms of network “assets” that may narrow scope of assessments
  - FCI/CUI assets
  - Security protection assets
  - Contractor risk managed assets
  - Specialized assets: Government property, IoT/OT, restricted information systems, test equipment

## Cybersecurity Maturity Model Certification (CMMC)

- ? Details of implementation
- ? Application to cloud environments
- ? Adoption by civilian agencies
- ? Impact on current cybersecurity obligations
- ? Viability v. effectiveness

## DOJ Civil Cyber-Fraud Initiative

- Announced October 2021
- Led by the Civil Division's Commercial Litigation Branch and Fraud Section
- Focused on prosecuting False Claims Act violations against government contractors that fail to follow cybersecurity contract requirements

## DOJ Civil Cyber-Fraud Initiative

### Three hooks:

1. Providing deficient cybersecurity products or services
2. Misrepresenting cybersecurity compliance
3. Failing to monitor and/or report cybersecurity incidents in accordance with contract requirements

## DOJ Civil Cyber-Fraud Initiative

### What's next?

- ↑ Growing resource allocation within government to investigate and prosecute FCA cyber claims
- ↑ Increased coordination within government
- ↑ Piqued interest in relators' bar for *qui tam* actions
- ↑ Uptick in investigations, settlements, and litigation

# DOJ Civil Cyber-Fraud Initiative

Improves  
cybersecurity  
practices/helps  
prevent cyber  
intrusions

Holds  
contractors &  
grantees to  
their  
commitments

Ensures a level  
playing field

Helps identify,  
create, &  
publicize  
patches for  
vulnerabilities

Reimburses  
taxpayers for  
losses

Credit for disclosure, remediation, and cooperation with  
ongoing government investigations

Pub K

PUBLIC CONTRACTS

## Privacy & Security

- Protecting Personally Identifiable Information
- The Privacy Act; applicability to contractors
  - ▷ FAR 52.224-1, Privacy Act Notification
  - ▷ FAR 52.224-2, Privacy Act
  - ▷ FAR 52.224-3, Privacy Training
- NIST SP 800-122, *Guide to Protecting the Confidentiality of PII*

# Cyber OT

## "Relevant Systems"

An offeror – where subject to NIST SP 800-171 – must have a current assessment "for *each* covered contractor information system that is *relevant* to the offer, contract, task order, or delivery order. DFARS 252.204-7019

Many companies have multiple systems.

Unclear which are "relevant."

Does DoD intend that the new self-assessment regime apply identically to factory systems (with ICS and manufacturing OT) as to IT systems?

## Where There is Alignment

Some factory systems use data in a CUI category (e.g., CTI), to control CNC machines.

Factory systems themselves can store, process, or transmit forms of CUI, and can be connected to other systems with CUI.

An adversary attack upon the factory systems could exfiltrate or compromise CUI and cause factory systems to fail or operate improperly.

Adversaries might exploit vulnerabilities in networked factory systems to reach, exfiltrate, or otherwise compromise CII on connected information systems.

## Potentially Extreme Choices

Replace OT Equipment? Too expensive for many DIB companies; many factories operate using "legacy" hardware and software; new systems capital-intensive; continuity impact.

Air Gap OT? Not an optimal solution; may improve -171 score but disrupt mfg process. Disconnecting factories would exclude use of sensor-informed CPS, IoT functionalities, and mfg retard transition to "Industry 4.0."

Form CDI "Enclaves"? Not simple technically; ~ infeasible for multi-customer factories; frustrates customer/client data exchange.



## IoT Cybersecurity Improvement Act of 2020

- Tasked NIST with developing standards and guidelines governing federal IoT device security
- Prohibits agencies from procuring, obtaining, or using IoT devices not in compliance with NIST's standards and guidelines
- Governs vulnerability disclosure process vis-à-vis federal agencies and contractors

## IoT Cybersecurity Improvement Act of 2020

- NIST published corresponding standards in November 2021:
  - NIST SP 800-213, *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*
  - NIST SP 800-213A, *IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog*



# Question Set 2

Event Sponsors

Platinum Sponsor

NICHOLS LIU

SERVING GOVERNMENT CONTRACTORS

Gold Sponsors

pillsbury

VENABLE LLP

Silver Sponsors

Arnold & Porter

MORRISON  
FOERSTER

COVINGTON

HK>A

Vinson & Elkins

wiley

BLANKROME  
CELEBRATING 75 YEARS

PILIERO  
MAZZA

DLA PIPER

crowell|moring

bakertilly

Holland & Knight

SheppardMullin

PERKINS coie  
COUNSEL TO GREAT COMPANIES

BRG  
Berkeley Research Group

GT GreenbergTraurig

JENNER & BLOCK

**Thank you!**

**See you tomorrow at 12:00 p.m. for  
Day 3 of Pub K's Annual Review 2022**



For more information  
Visit <https://pubkgroup.com/features/>

