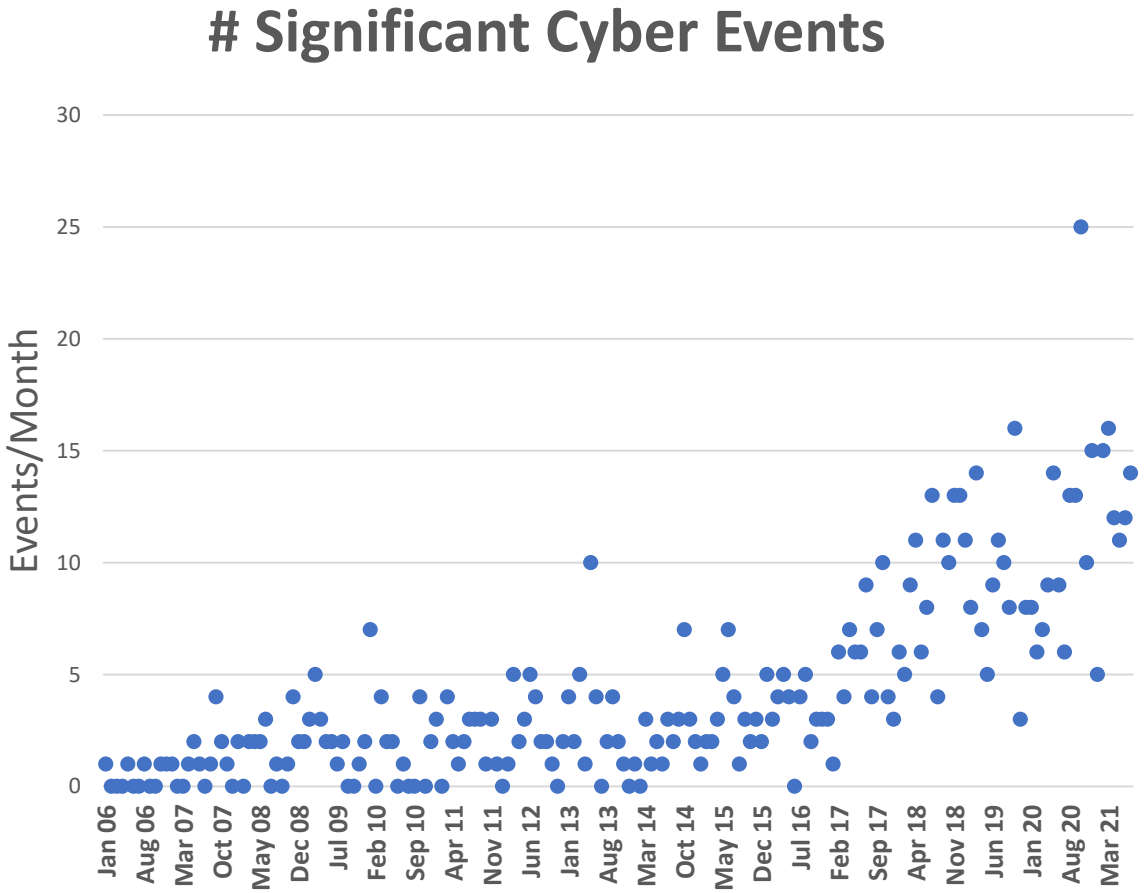
EO14028: Improving the Nation's Cybersecurity

Supply Chain Cybersecurity is More than Just CMMC

Gordon Bitko
Senior Vice President, Public Sector
Gbitko@itic.org

Why EO 14028?

Image Credit: David Wolpoff



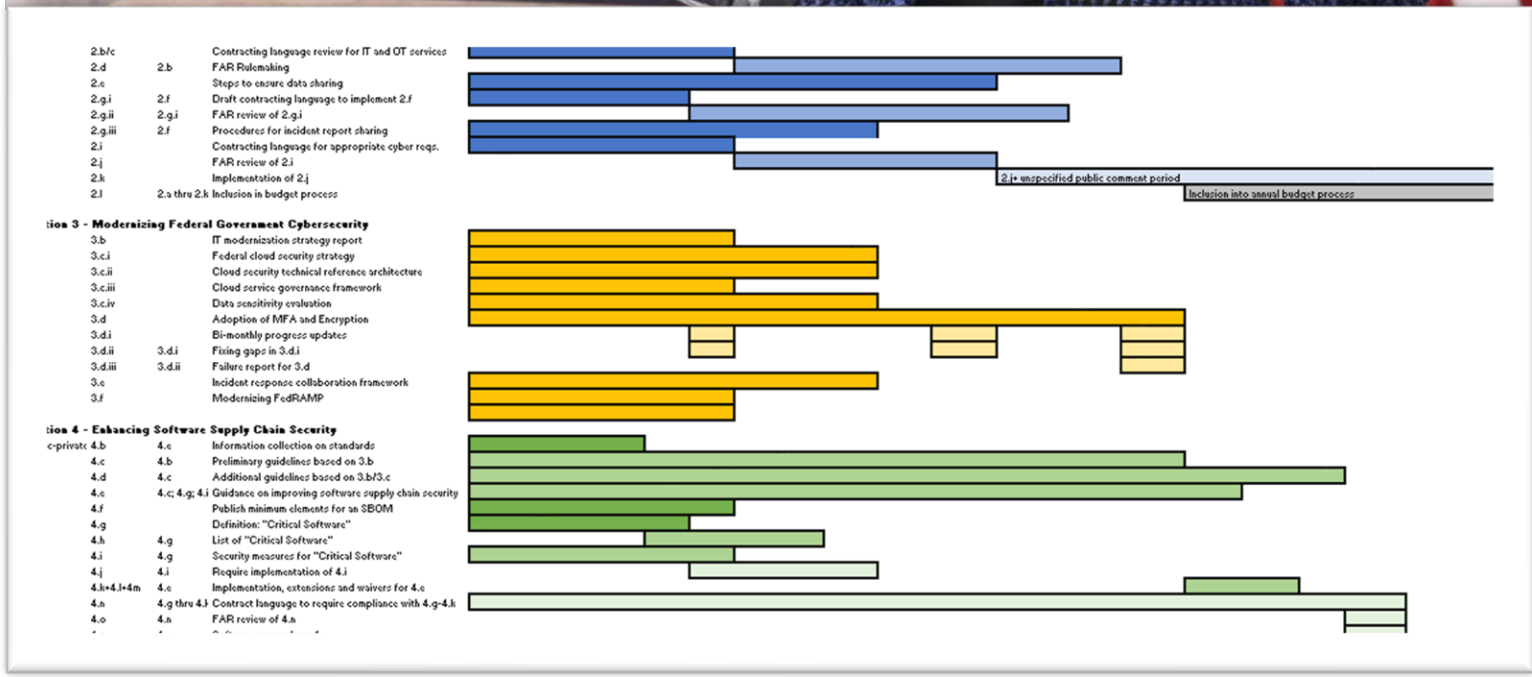
Data per CSIS timeline of Significant Cyber Incidents
https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
Significant: "cyber attacks on government agencies, defense and high tech companies, or economic crimes with losses of more than a million dollars"

ITI

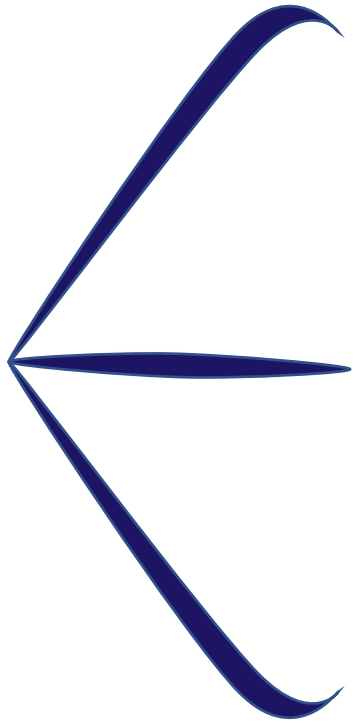
What is EO14028?

Whole of government risk management – Executive Order 14028 – May 12, 2021

- Prioritizes prevention, detection, assessment and remediation of cyber incidents
- USG should lead by example, and public/private partnership is required
- Requirements of the EO apply to all Federal Information Systems (OT and IT)



Key Pillars in EO 14028



Supplier Accountability

- Section 4: Enhancing Software Supply Chain Security

Intelligence Driven Operations

- Section 2: Removing Barriers to Sharing Threat Information
- Section 8: Improving the Federal Government's Investigative and Remediation Capabilities

Better risk management in the .gov

- Section 3: Modernizing Federal Government Cybersecurity
- Section 6: Standardizing the Federal Government's [incident response] Playbook

Relevant EO Deliverables

Standards for secure software development
Critical Software definition and controls
Mandatory threat and incident reporting and sharing
Mandatory logging requirements
Tech modernization: Zero Trust, secure clouds + FedRAMP, encryption, increased automation of services
Consistency in agency incident response per NIST standards

ITI

Immediate Supply Chain Impact of EO 14028

Open FAR Cases as of 7/30/2021

Case Number	Part Number	Title	Synopsis	Status
2021-019		Standardizing Cybersecurity Requirements for Unclassified Information Systems	Amends the FAR to standardize common cybersecurity contractual requirements across Federal agencies for unclassified information systems, pursuant to Department of Homeland Security recommendations in accordance with sections 2(i) and 8(b) of Executive Order 14028, Improving the Nation's Cybersecurity.	06/11/2021 Case on hold, pending DHS recommendations.
2021-018		Reporting Cyber Incidents Involving Software Products or Services	Amends the FAR to require contractors providing software products or services report cyber incidents to the federal government to facilitate effective cyber incident response and remediation, pursuant to Department of Homeland Security recommendations in accordance with sections 2 (g)(i) and 8(b) of Executive Order 14028, Improving the Nation's Cybersecurity.	06/11/2021 Case on hold, pending OMB and DHS recommendations.
2021-017		Sharing Cyber Threat and Incident Information	Amends the FAR to increase the sharing of information about cyber threats and incident information between the Government and information technology and operational technology service providers, pursuant to: OMB recommendations, in accordance with section 2(b)-(c), and Department of Homeland Security recommendations, in accordance with section 8(b), of Executive Order 14028, Improving the Nation's Cybersecurity.	06/11/2021 Case on hold, pending DHS recommendations.

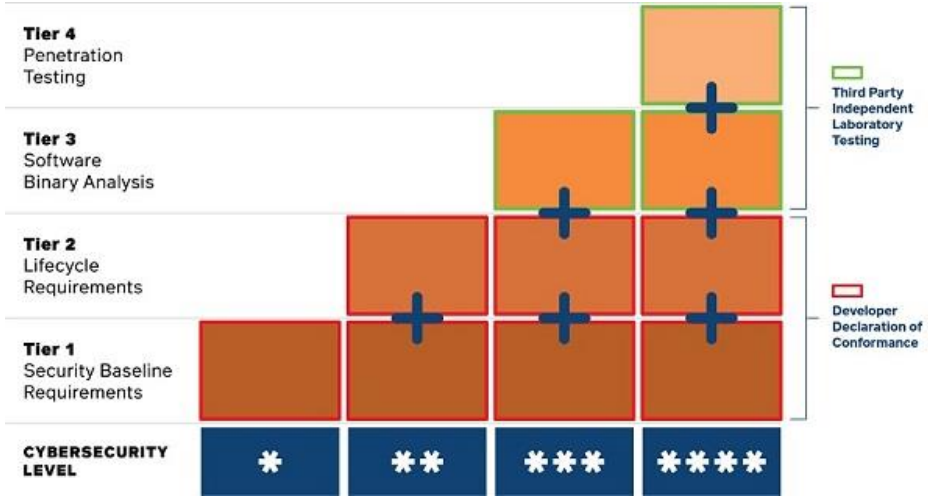
ITI

Indirect Supply Chain Implications of EO 14028

Issue: EO provisions may be applied more broadly

Example: EO 4.s-4.v Software labeling pilot – Initial focus is on Consumer IOT products

Cybersecurity Labelling Scheme
BY CYBER SECURITY AGENCY OF SINGAPORE



Considerations for NIST:

- Align labelling with international standards and best practices
- Grant conformity assessment reciprocity

ITI

CMMC/DFARS 7012 and EO14028 Need Harmonization

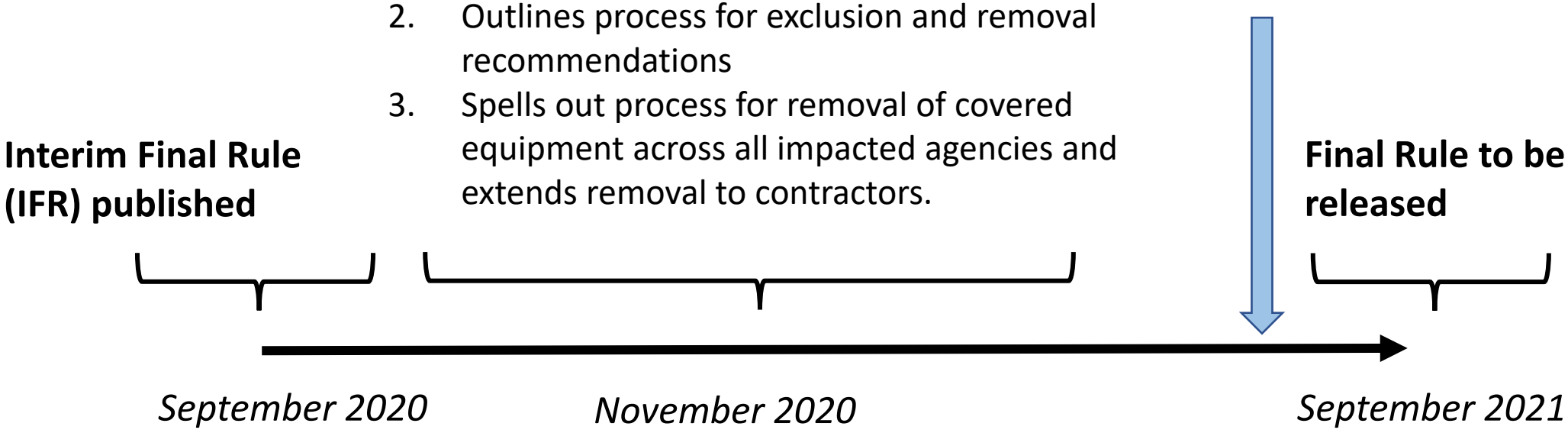
	CMMC/DFARS Control/Clause	EO
Software development/ Source code verification	CA.3.162 (L3): Employ a security assessment of enterprise software that has been developed internally (i.e., code review)	4(e): Minimum Standard for Vendor or Developer Verification of Software: Threat Modeling, Automated Testing, Static Analysis, etc. Note: Currently these are voluntary but expect mandates per 4(j).
Incident reporting	7012.(c).(1): A covered cyber incident is to be rapidly reported through dibnet.dod.mil	2(f): ICT contractors must promptly report incidents to the involved agency and CISA – details pending FAR 2021-018 update
Logging standards	Multiple domains, including Audit & Accountability and Incident Response	Sec. 8: Policies for logging, retention, management, access and sharing- details pending OMB/Federal CIO/CISO guidance
Zero Trust Architecture	Multiple domains, including Access Control, Configuration Management, Identification and Authentication	Sec 3: Each agency shall develop a plan to implement Zero Trust Architecture

ITI

Federal Acquisition Supply Chain Security Act

Key Points of the IFR

1. Creates an information sharing Task Force to develop procedures on submission of supply chain risk information
2. Outlines process for exclusion and removal recommendations
3. Spells out process for removal of covered equipment across all impacted agencies and extends removal to contractors.



ITI

Questions?