CAKE Talk: SCRM & C-SCRM

Continuous Assessment, Knowledge, and Education

Ms. Julienne Picot Chappell, SAF/CNZP

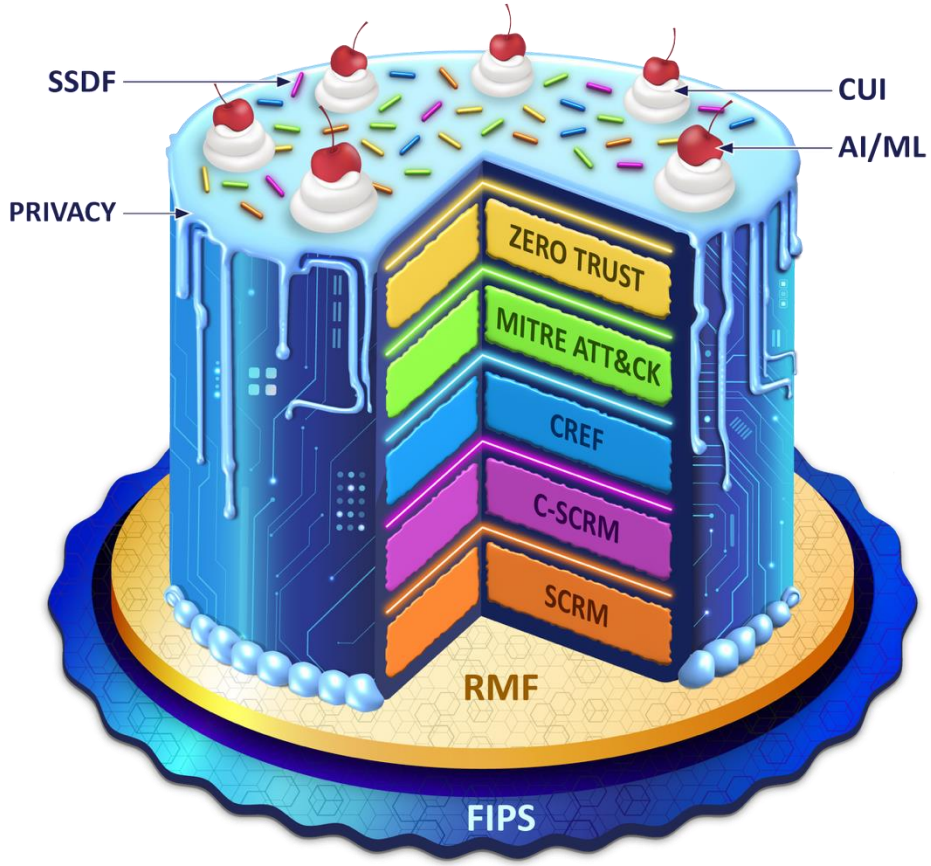
Ms. Brandy Barrere, SAF/AQRS

Topics

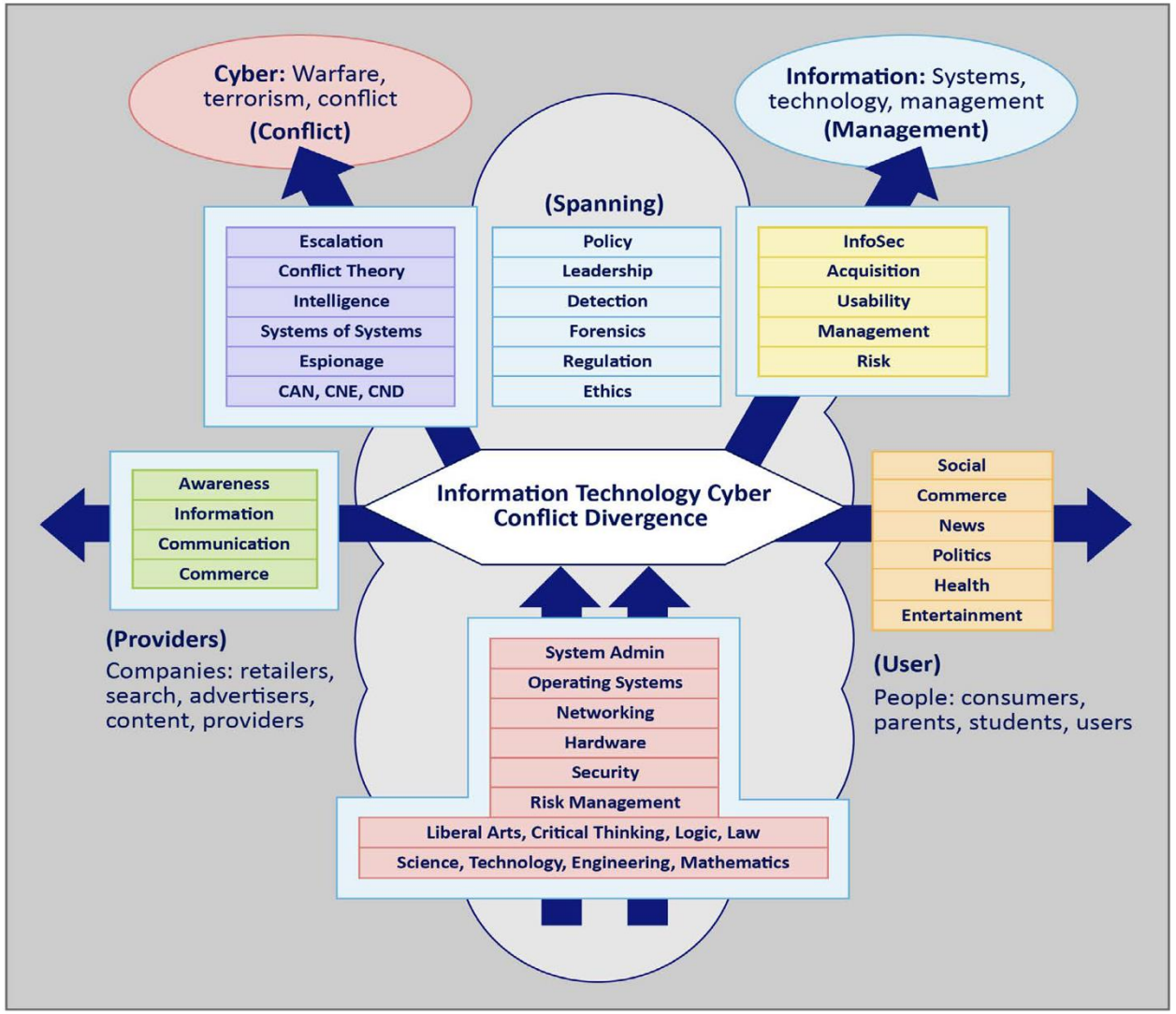
- Cyber CAKE, DAFITC 1st Anniversary De-Frost
- Layer 1 Flavor Profile: Supply Chain Risk Management (SCRM)
  - Defining Supply Chain and SCRM
  - SCRM Risk Lenses
- Layer 2 Flavor Profile: Cyber SCRM (C-SCRM)
  - Acquisition Intersections
  - NIST Cybersecurity Framework (CSF) 2.0 C-SCRM Govern Function

What is the Cyber CAKE?

- Continuous Assessment, Knowledge, and Education (CAKE)
- The Cyber CAKE concept provides a structured, transparent framework that demystifies cybersecurity
- Easy to understand, relatable, useful analogies convey core cybersecurity concepts
- Each layer represents foundation elements of cybersecurity and offers tangible practitioner strategies for grasping the “why” and confidently implement and assess cyber strategies
- Aligned to the Cybersecurity Awareness and Training category within the **Protect** function of the NIST Cybersecurity Framework 2.0 with relevant core “Cookbooks” cited and referenced throughout
- The result of the Cyber CAKE concept is “baked in cybersecurity” and compliance used as strategy to measure resilience



Why the Cyber CAKE?



- Cyberspace is a complex, multidimensional domain that encompasses not only conflict, but also communication, commerce, and societal development
- The knowledge base is inherently fragmented
- There is no true cyberspace "expert"
- Need: transform a daunting obstacle course into a series of manageable steps

Supply Chain Risk Management (SCRM)

Cyber Cake Layer 1

Supply Chain

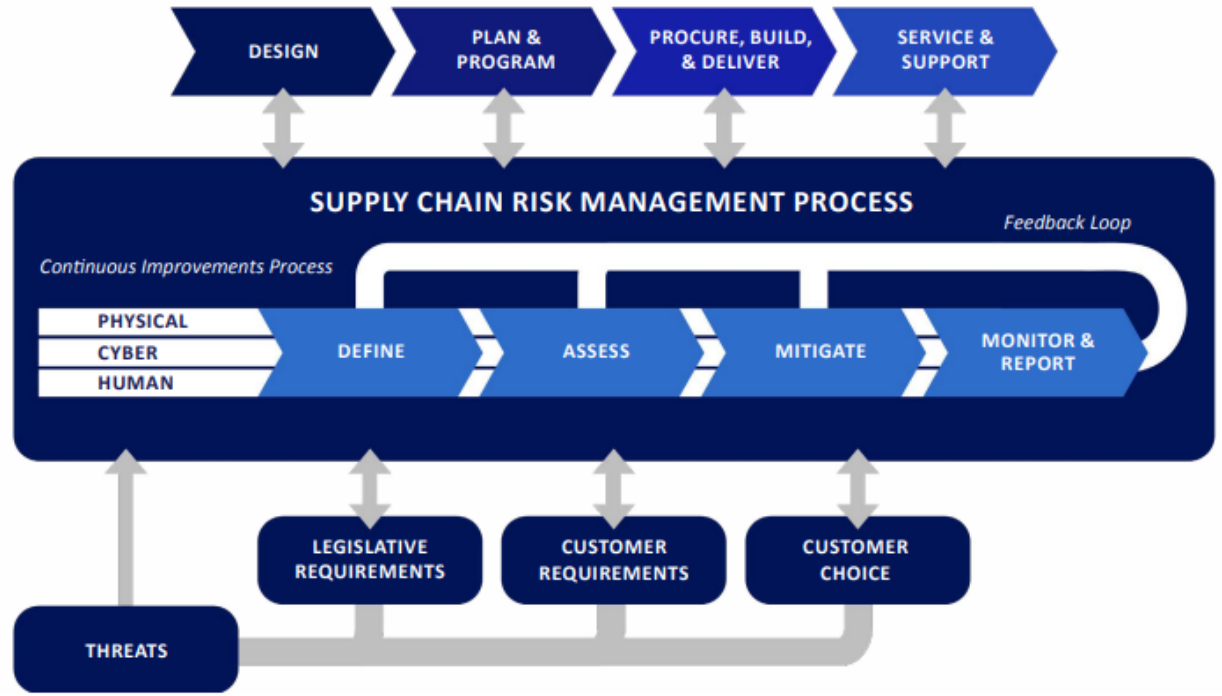
- The linked activities associated with providing materiel to end users for consumption. Those activities include supply activities (such as organic and commercial inventory control points (ICPs) and retail supply activities), maintenance activities (such as organic and commercial depot level maintenance facilities and intermediate repair activities), and distribution activities (such as distribution depots and other storage locations, container consolidation points, ports of embarkation and debarkation, and ground, air, and ocean transporters). (DoDI 4140.01)
- The linked activities associated with providing materiel from a raw material stage to an end user as a finished product in its final disposition. (DAFPD23-1)
- The term supply chain refers to the linked set of resources and processes between and among multiple levels of an enterprise, each of which is an acquirer that begins with the sourcing of products and services and extends through the product and service life cycle. (NIST SP800-161r1-upd1)
- A linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer. (OMB Circular A-130/CNSSI 4009 dtd 3/2/22)

Supply Chain Risk

- Supply chain risk is anything that has potential to jeopardize the integrity of products, services, people and technologies or disrupt the flow of product, materiel, information, and finances across the life cycle of a weapon or support system. (DAFI20-101/63-101)
- Risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. (OMB Circular A-130/CNSSI 4009 dtd 3/2/22)
- The risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of an item of supply or a system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of a system (referenced from The Ike Skelton National Defense Authorization Act for Fiscal Year 2011, Section 806). (CNSSD No. 505/CNSSI 4009 dtd 3/2/22)

Supply Chain Risk Management (SCRM)

- The systematic process for managing risk by identifying, assessing, and mitigating actual or potential threats, vulnerabilities, and disruptions to the DAF supply chain from beginning to end to ensure mission effectiveness. (DAFPD23-1)
- The process for managing risk by identifying, assessing, and mitigating threats, vulnerabilities, and disruptions to the DoD supply chain from beginning to end to ensure mission effectiveness. (DoDI 4140.01)

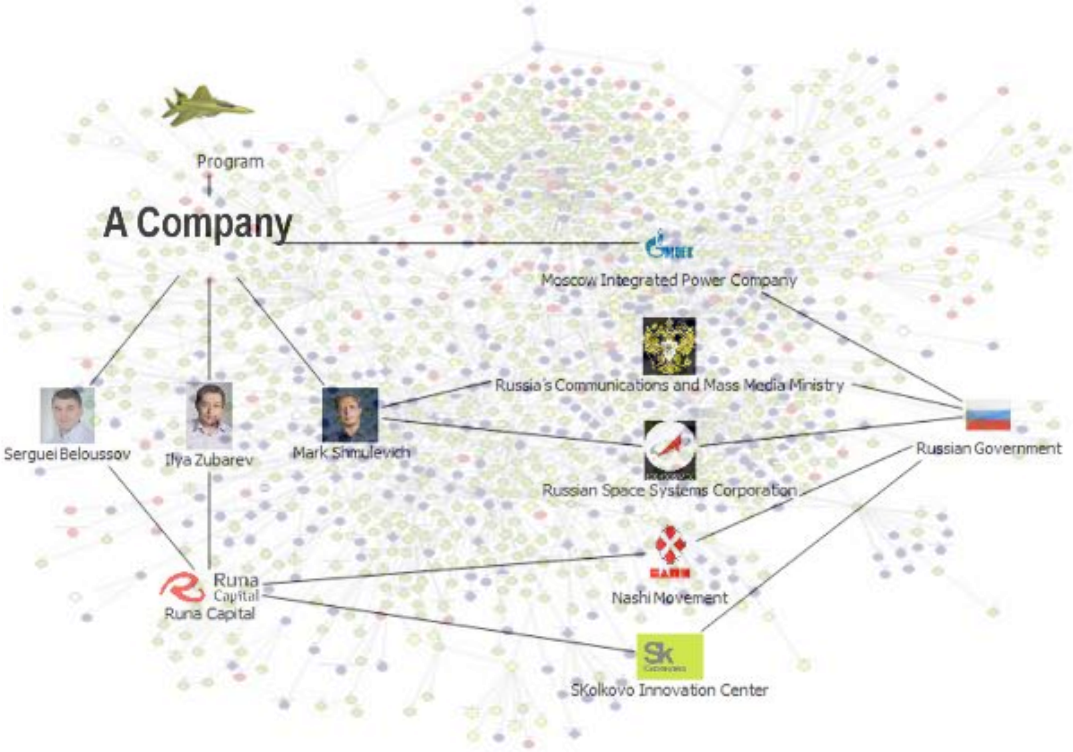


Supply Chain Risk Lenses

- Product Quality/Counterfeit: material discrepancies
- Financial: distressed suppliers, currency exchange volatility
- Political and regulatory: includes political unrest, terrorism, new laws or regulations
- Industry Operations: disputes, business ethics
- Environmental: includes natural disasters, man-made disasters like fires, and Pandemics
- Technology: disruptive growth, data and cyber breaches, tech insertion, Intellectual Property laws, operational supply base risk: diminishing manufacturing supply and material shortages (DMSMS)
- Human Capitol: health and safety, workforce shortage
- Foreign influence: investment, weaponized mergers & acquisitions

Complexity

- System interdependencies increase Enterprise risk exposure
- Massive, complex, geographically disbursed, multi-tiered supply chains
  - Thousands of entities, large supplier eco systems
  - Multi-hemispheric, widely dispersed supply chains
    - A Company - example down to 4th tier
    - Suppliers are plotted across the globe and each of these suppliers are assessed through the 8 SCRM lenses to identify risks to the weapons systems
    - Red dots on the map indicate a high risk throughout exposure



SCRM in Practice

- Framework for developing, improving, and conducting management activities, in order to plan, source, make, deliver, and maintain materiel
- Emphasizes supply chain responsiveness and prudent stewardship in supply chain activities
- Consider all life cycle costs associated with materiel management, including acquiring, distributing, transporting, storing, maintaining, repairing, protecting, and disposing
- Integrated Life Cycle Management is the process that encompasses all phases and functions (requirements identification, development, testing, fielding, product support, and disposal) necessary for effective acquisition and sustainment of systems, subsystems, end items, and services to satisfy valid warfighter capability needs. (AFPD20-1/AFPD63-1)

Supply Chain Infiltration Examples

- Weaponized mergers
- Foreign governments' cornering rare earth element markets
- Cyber, software & hardware attacks
  - Commercial entity exploitation (IP, tech transfer, counterfeit parts)
- Controlling infrastructure (e.g. ports) via targeted ownership

Integrated Life Cycle Management

- (DAFI 63-101/20-101) Directive overarching processes and procedures required to deliver and sustain warfighting capabilities
- Integrated Life Cycle Management governs all aspects of infrastructure, resource management, and business systems necessary for the successful acquisition of systems, subsystems, end items, and services to satisfy validated warfighter or user requirements
- Program Protection Planning (PPP)
  - Identify critical program information, critical mission functions, and critical component to prioritize efforts
  - All-source threat assessments on critical components per DoDI 5200.44 and DoDI 5000.83_DAFI 63-113, and assessments of sub-tiers in the prime contractor supply chain.
  - Conduct industrial base constraints and supply chain assessments
  - Independent supply chain risk reviews
- Include SCRM requirements in market research, RFPs, contract language, and source selection evaluation criteria
- Integrate identified risks into program risk management activities

Program Protection Plan

- Program protection is a multi-functional activity to plan for and integrate holistic security policies and practices throughout the integrated life cycle.
- Ensure critical program information and mission critical functions and components are protected to keep technological advantages in and malicious content out.

- Communications Security (COMSEC) countermeasures
- Anti-tamper
- Operations Security (OPSEC)
- Counterintelligence
- Foreign Intelligence
- System Security Engineering
- Trusted Systems and Networks (TSN)
- Acquisition Security
- Cybersecurity
- Nuclear Systems Security
- Physical Security
- SCRM
- C-SCRM
- Assurance

Cyber Supply Chain Risk Management (C-SCRM)

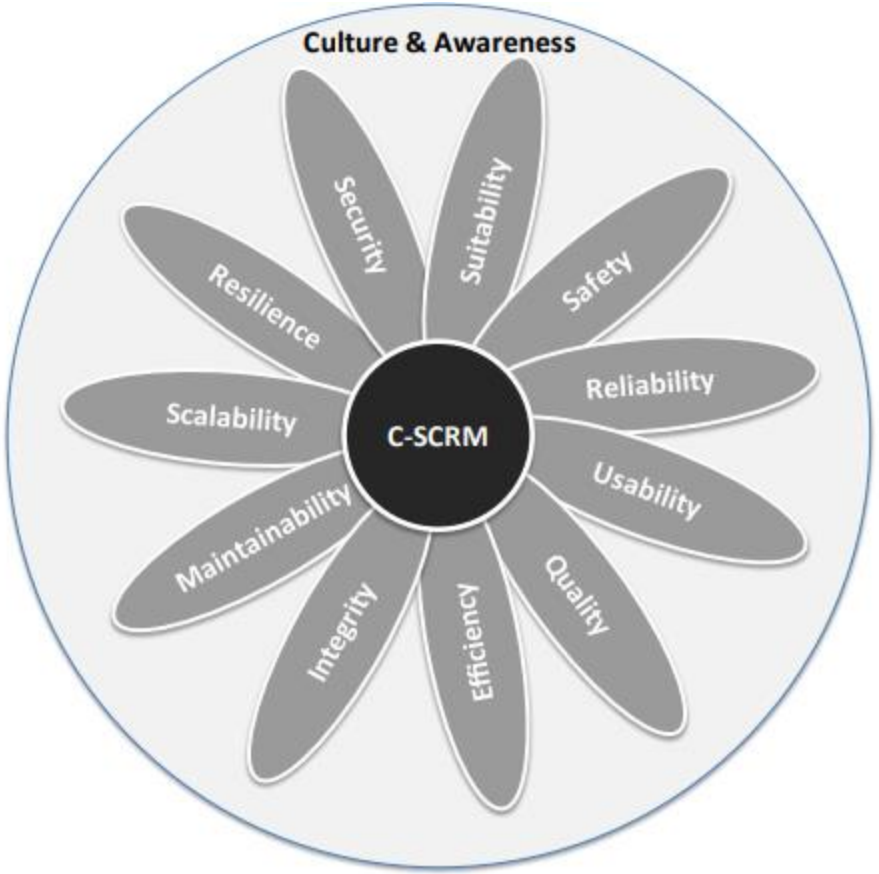
Cyber Cake Layer 2

Cyber Supply Chain Risk Management (C-SCRM)

- Cybersecurity risks throughout the supply chain refers to the potential for cyber compromise or harm that may arise from suppliers, their supply chains, their products, or their services.
- C-SCRM is the organized and purposeful management of cybersecurity risks throughout the supply chain.
  - The strategy and methods for protecting critical defense information and Information and Communications Technology (ICT) from supply chain exploits in a cyber-contested operational environment.
  - C-SCRM in practice: mitigates potential exploitation of vulnerabilities or exposures within products and services that traverse the supply chain or threats that exploit vulnerabilities or exposures within the supply chain itself.
- Cyber exploit differentiation:
  - Cyber attack – gaining unauthorized access by exploiting a system vulnerability, via methods such as hacking, malware, phishing, insider access, etc.
  - Supply Chain attack – targeting sub-tier vendors or third-party suppliers in order to compromise an ICT product or system prior to delivery

12 Dimensions of C-SCRM

C-SCRM requires enterprise recognition and awareness, and it lies at the intersections of security, suitability, safety, reliability, usability, quality, integrity, efficiency, maintainability, scalability, and resilience.



CSF 2.0 Govern – Supply Chain (GV.SC) 1-5

- GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders
- GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally
- GV.SC-03: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes
- GV.SC-04: Suppliers are known and prioritized by criticality
- GV.SC-05: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties

CSF 2.0 Govern – Supply Chain (GV.SC) 6-10

- GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships
- GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship
- GV.SC-08: Relevant suppliers and other third parties are included in incident planning, response, and recovery activities
- GV.SC-09: Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle
- GV.SC-10: Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement

FISMA FY2025

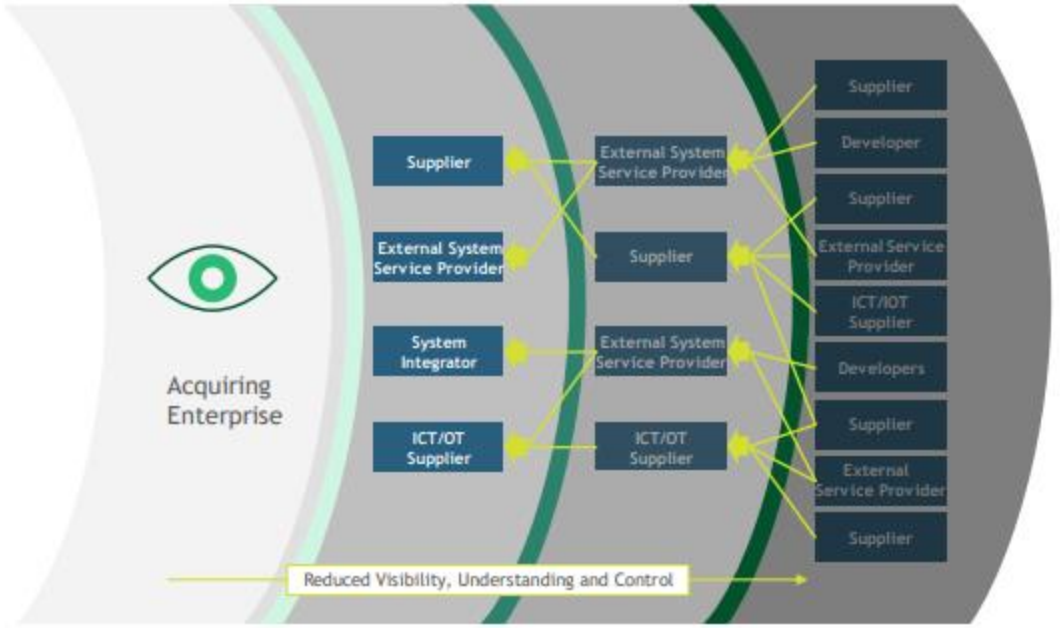
- Maturity Levels: Ad Hoc – Defined – Consistently Implemented – Managed and Measurable – Optimized
- To what extent does the organization ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain requirements?
  - The organization has defined and communicated policies and procedures to ensure that [organizationally defined products, system components, systems, and services] adhere to its cybersecurity and supply chain risk management requirements. The following components, at a minimum, are defined:
    - The identification and prioritization of externally provided systems, system components, and services as well how the organization maintains awareness of its upstream suppliers.
    - Integration of acquisition processes, including the use of contractual agreements that stipulate appropriate C-SCRM measures for external providers.
    - Tools and techniques to use the acquisition process to protect the supply chain, including, risk-based processes for evaluating cyber supply chain risks associated with third party providers, as appropriate. Contract tools or procurement methods to confirm contractors are meeting their contractual C-SCRM obligations.
- The organization analyzes, in a near-real time basis, the impact of material changes to C-SCRM assurance requirements on its relationships with external providers and ensures that acquisition tools, methods, and processes are updated as soon as possible.

Operational C-SCRM

- Assemble a plan focused on achieving desired C-SCRM outcomes.
  - Focus on managing operational-level risk exposure resulting from any ICT/OT related products and services provided through the supply chain that are in use by the system or fall within the scope of the system authorization boundary.
- Address C-SCRM requirements in Acquisition activities involving procurement and contract management
  - Avoid using generalized requirements statements, such as “ensure compliance with NIST SP 800-161, Rev. 1 controls.”
  - Select controls relevant to the specific use case of the service or product being acquired
- Assign C-SCRM roles and functional responsibilities for key personnel (minimally, define team roles, followed by IT Security personnel, then acquisition workforce)
- Identify known and potential threat vectors
  - Identify internal and external information sources for threat identification and assessments
  - Analyze the likelihood and impact of potential supply chain cybersecurity threats exploiting an operational-level vulnerability (e.g., in a system or system component)

Acquisition Intersections

- Maintain a current and accurate inventory of the program's supplier relationships, contracts, and any products or services those suppliers provide.
  - Facilitates analysis and understanding of the exposure to cybersecurity risks throughout the supply chain
  - Helps to focus attention and assign priority to critical suppliers of the most strategic or operational importance to the program
- Identify products and services requiring a higher level of confidence in risk mitigation and areas of risk, such as overreliance on a single source of supply.
- Inventory and supplier mapping facilitates the selection and tailoring of C-SCRM contract language and evaluation criteria.
- Relevant controls SA-1, SA-2, SA-4, SR-5, SR-13 of NIST SP 800-53, Rev. 5.

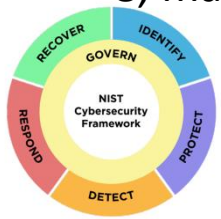


Acquisition Intersections

Source of Supply, Product, or Service Characteristics	Risk Indicators, Analysis, and Findings
• Features and functionality • Access to data and information, including system privileges • Installation or operating environment • Security, authenticity, and integrity of a given product or service and the associated supply and compilation chain • The ability of the source to produce and deliver a product or service as expected • Foreign control of or influence over the source (e.g., foreign ownership, personal and professional ties between the source and any foreign entity, legal regime of any foreign country in which the source is headquartered or conducts operations*) • Market alternatives to the source • Provenance and pedigree of components • Supply chain relationships and locations • Potential risk factors, such as geopolitical, legal, managerial/internal controls, financial stability, cyber incidents, personal and physical security, or any other information that would factor into an analysis of the security, safety, integrity, resilience, reliability, quality, trustworthiness, or authenticity of a product, service, or source	• Threat information includes indicators (system artifacts or observables associated with an attack), tactics, techniques, and procedures (TTPs) • Security alerts or threat intelligence reports • Implications to national security, homeland security, national critical infrastructure, or the processes associated with the use of the product or service • Vulnerability of federal systems, programs, or facilities • Threat level and vulnerability level assessment/score • Potential impact or harm caused by the possible loss, damage, or compromise of a product, material, or service to an enterprise's operations or mission and the likelihood of a potential impact, harm, or the exploitability of a system • The capacity to mitigate risks is identified

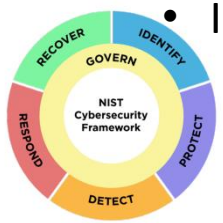
NIST SP800-53r5 Control Highlights

- RA-2 Security Categorization; Level(s): 1, 2, 3; Related Controls: RA-9
  - Categorize the system and information it processes, stores, and transmits
  - Document the security categorization results, including supporting rationale, in the security plan for the system; and
  - Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision
- Security categorization is critical to C-SCRM at Levels 1, 2, and 3
  - In addition to [FIPS199] categorization, security categorization for C-SCRM should be based on the criticality analysis that is performed as part of the Software Development Life Cycle (SDLC).
  - RA-2 contributes to flaw identification/remediation, root cause analysis, secured logging and other SCRM activities.
- Security categories describe the potential adverse impacts or negative consequences to organizational operations, organizational assets, and individuals if organizational information and systems are compromised through a loss of confidentiality, integrity, or availability.
- Security categorization processes facilitate the development of inventories of information assets and, along with CM-8, mappings to specific system components where information is processed, stored, or transmitted.



NIST SP800-53r5 Control Highlights

- PM-30 Supply Chain Risk Management Strategy; Level(s): 1, 2; Related Controls: PL-2
  - Select and document baseline C- SCRM controls that address enterprise, program, and system-specific needs
  - Require prime contractors to implement controls and flow down requirements to relevant sub-tier contractors
- PM-31 Continuous Monitoring Strategy; Level(s): 1, 2, 3; Related Controls: PM-30
  - The continuous monitoring strategy and program should integrate C-SCRM controls at Levels 1, 2, and 3
- RA-10 Threat Hunting; Level(s): 1, 2, 3
  - Enterprises should actively monitor for threats to their supply chain. This requires a collaborative effort between CSCRM and other cyber defense-oriented functions within the enterprise
- SA-1 Policy and Procedures; Level(s): 1, 2, 3
  - C-SCRM procurement actions and contracts include requirements language or clauses that address which controls are mandatory or desirable and may include implementation specifications
- SA-2 Allocation of Resources; Level(s): 1, 2
  - Incorporate C-SCRM requirements when determining and establishing the allocation of resources
- SA-4 Acquisition Process; Level(s): 1, 2, 3; Related Controls: SA-4 (1), (2), (3), (6), and (7)
  - Include C-SCRM requirements, descriptions, and criteria in applicable contractual agreements



NIST SP800-53r5 SR Family Highlights

- SR-4 Provenance; Level(s): 2, 3
  - Provenance should be documented for systems, system components, and associated data throughout the SDLC. Enterprises should consider producing SBOMs for applicable and appropriate classes of software, including purchased software, open source software, and in-house software.
- SR-5 Acquisition Strategy, Tools, and Methods; Level(s): 1, 2, 3; Related Controls: SA Control Family
  - Refer to NIST SP800-161r1-upd1 section 3, Appendix F, and SA family controls for supplemental C-SCRM guidance
- SR-6 Supplier Assessments and Reviews; Level(s): 2, 3
  - Assessments any information pertinent to the security, integrity, resilience, quality, trustworthiness, or authenticity of the supplier or their provided services or products. Enterprises should consider applying this information against a consistent set of core baseline factors and assessment criteria to facilitate equitable comparison (between suppliers and over time).
- (New) SR-13 Supplier Inventory; Level(s): 2, 3; Related Controls: RA-9
  - Some suppliers are more critical than others, based on the criticality of missions, functions, programs, projects,
  - Enterprises should use criticality analysis to help determine which products and services are critical to determine the criticality of suppliers to be documented in the supplier inventory.

C-SCRM Plan

- The C-SCRM plan developed at Tier 3 is implementation-specific and provides policy implementation, requirements, constraints, and implications.
- It can either be stand-alone or a component of a system security and privacy plan.
  - If incorporated, the C-SCRM components must be clearly discernable.
- The C-SCRM plan addresses the management, implementation, and monitoring of C-SCRM controls and the development and sustainment of systems across the SDLC to support mission and business functions
- Enterprises can leverage automated tools to ensure that all relevant sections of the C-SCRM plan are captured.
  - Automated tools can help document C-SCRM plan information, such as component inventories, individuals filling roles, security control implementation information, system diagrams, supply chain component criticality, and interdependencies
  - Near horizon: eMASS CR – Auto-build the C-SCRM Plan from A&A package contents

C-SCRM Plan Template

- System name and identifier
- System description
- Information types and categorizations
- Operational status
- Architecture diagram/boundary
- Inventory
- External information exchange/connections
- C-SCRM security controls in system baseline
- C-SCRM roles
- Continuity
- System applicable Laws/Regs/Policies

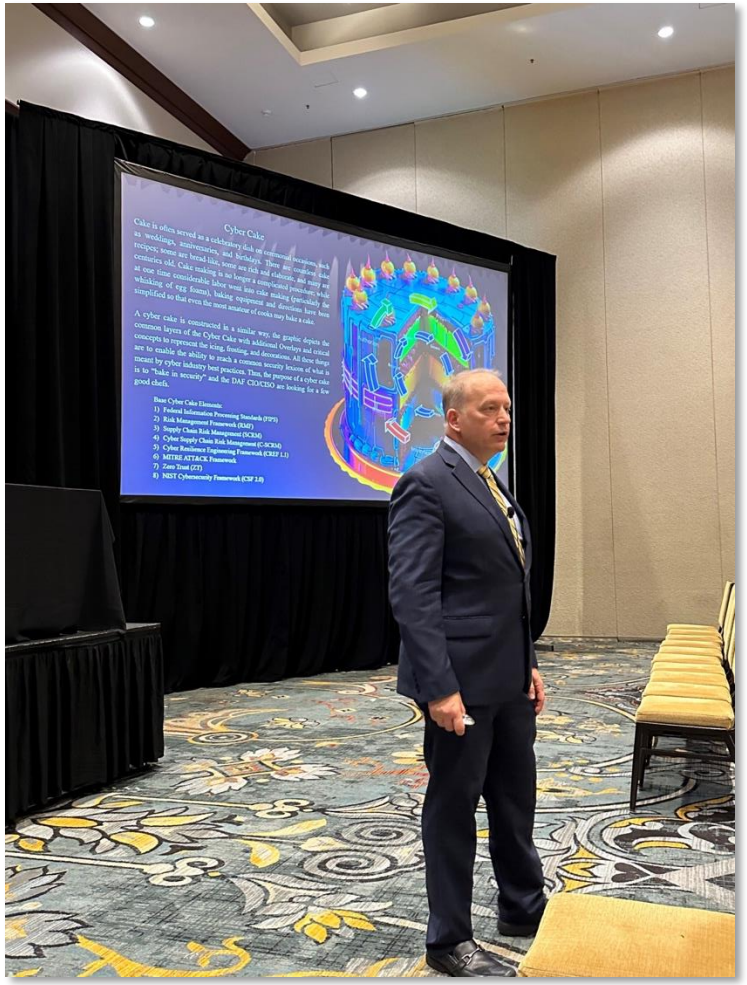
Questions?

julienne.chappell@us.af.mil

brandy.barrere@us.af.mil

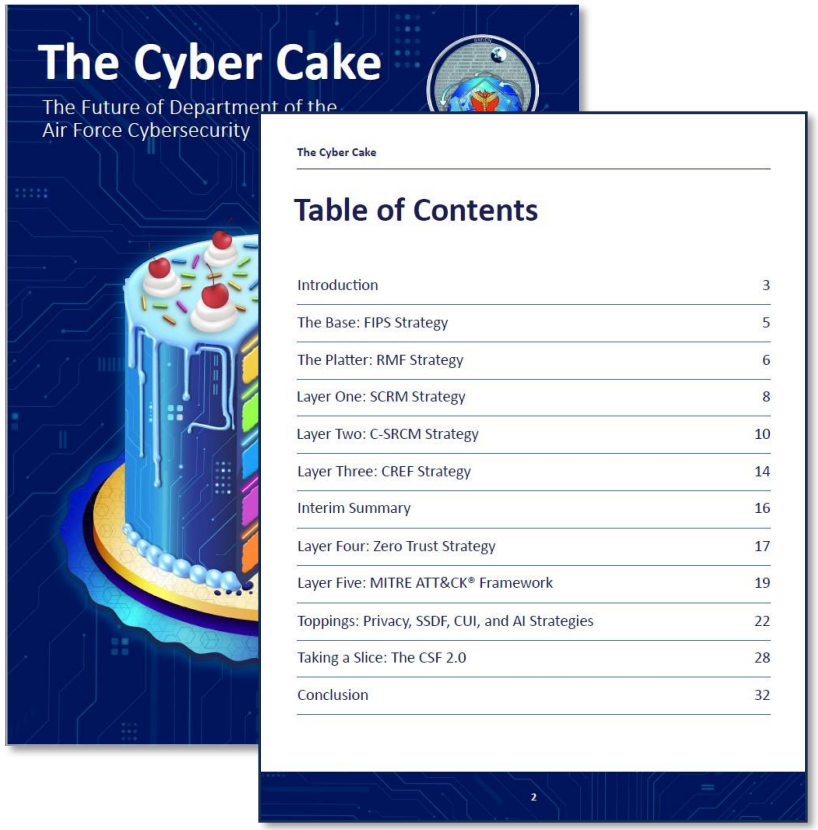
Background

- Challenge for DAFITC 2024 from CISO – How do we let the masses know that there is a way to do cybersecurity in a way that can be easily understood?
- Five breakout sessions:
  - The Cyber Cake – The Future of DAF Cybersecurity (opening)
  - Cake Baking 101 – Recipe
  - Cake Baking 201 – Prep
  - Cake Baking 301 – Assemble
  - Cake Baking 401 – Serve



Cyber Cake Materials

- 32-page comprehensive and foundational document*
- Each layer described in depth with corresponding figures and graphics for ease of reading



- 10-slide executive brief
- Presents highlights of Cyber Cake document for quick reading and reference

*all Cyber Cake content is Unclassified and derived from public sources

C-SCRM or ICT SCRM?

- C-SCRM is inclusive of ICT SCRM
  - Requires visibility into, understanding of, and control over cyber-supply risk management processes, as well as the decisions involved in developing and delivering ICT products and services.
- ICT includes all categories of ubiquitous technology used for gathering, storing, transmitting, retrieving, or processing of information (e.g., microelectronics, printed circuit boards, computing systems, software, signal processors, mobile telephony, satellite communications, and networks)
  - ICT is not limited to information technology (IT), as defined in section 11101 of title 40 of United States Code (USC). Rather, the term, ICT, reflects the convergence of IT and communications, as defined in DoD Instruction 5200.44.
- NIST has intentionally moved away from the term “ICT supply chain” as cybersecurity risks can arise in all product and service supply chains, including both ICT and non-technology supply chains.

Brownie Craft Cake – Recipe

This cake takes some time craft – at least ½ a day – but it's a great cake for a Minecraft themed party.

- Brownies (x3)
  - 1/3 cup vegetable oil (use extra virgin olive oil)
  - 1 eggs
  - 1/3 cup water
  - 1 Ghirardelli Brownie mix packs

- Make three 8x8 or 9x9 pans of brownies per box instructions (combine liquids, add brownie mix, cook at 325 degrees for 50min)
- Allow brownies to cool completely
- Remove from pan in one piece (silicone baking pans make this really easy: loosen brownie sides with a butter knife, place upside down on parchment paper, flip the pan sides inside out, loosen the "top" with a knife and pull the pan off without brownie bits)

- Fudge Icing (x2 if making a block)
  - 3 cups granulated sugar
  - 3 Tbsp light corn syrup
  - 1 cup milk
  - 4oz (squares) unsweetened chocolate
  - 1/3 cup butter
  - 1 tsp vanilla extract

- Cook sugar, syrup, milk and chocolate, stirring, until the sugar dissolves. Continue cooking to 232 ° F. (the syrup forms a very soft ball in cold water) stir occasionally to prevent scorching
- Remove from heat, add the butter, and cool without stirring until the bottom of the saucepan feels lukewarm.
- Add the vanilla and beat until the frosting is creamy and barely holds its shape. Spread quickly before the cake before the frosting hardens. * This never seems to harden * Layer Icing about 1cm thick between brownie
  - If frosting won't harden: refrigerate 6hrs to overnight, allow to stand at room temp for 5-10 minutes until softened enough to spread, then ice the brownie layers.

- Ganache Grass Top
  - 24oz white chocolate chips
  - 8oz heavy whipping cream
  - Green food coloring gel

- Soften chips in microwave for 1min - bring whipping cream to simmer
- Pour cream over chips, fully cover and let stand for 5-10m, whisk gently to combine
- Chill until ganache firms to the consistency of peanut butter (about 1 hour in a flat cake pan)
- Add food coloring to desired tint, stir to combine
- Spread over cake top and a "bit" over the edges