

U.S. General Services Administration

**Federal Acquisition Service
Information Technology Category
IT Security Subcategory**

presented by

Shon Lyublanovits

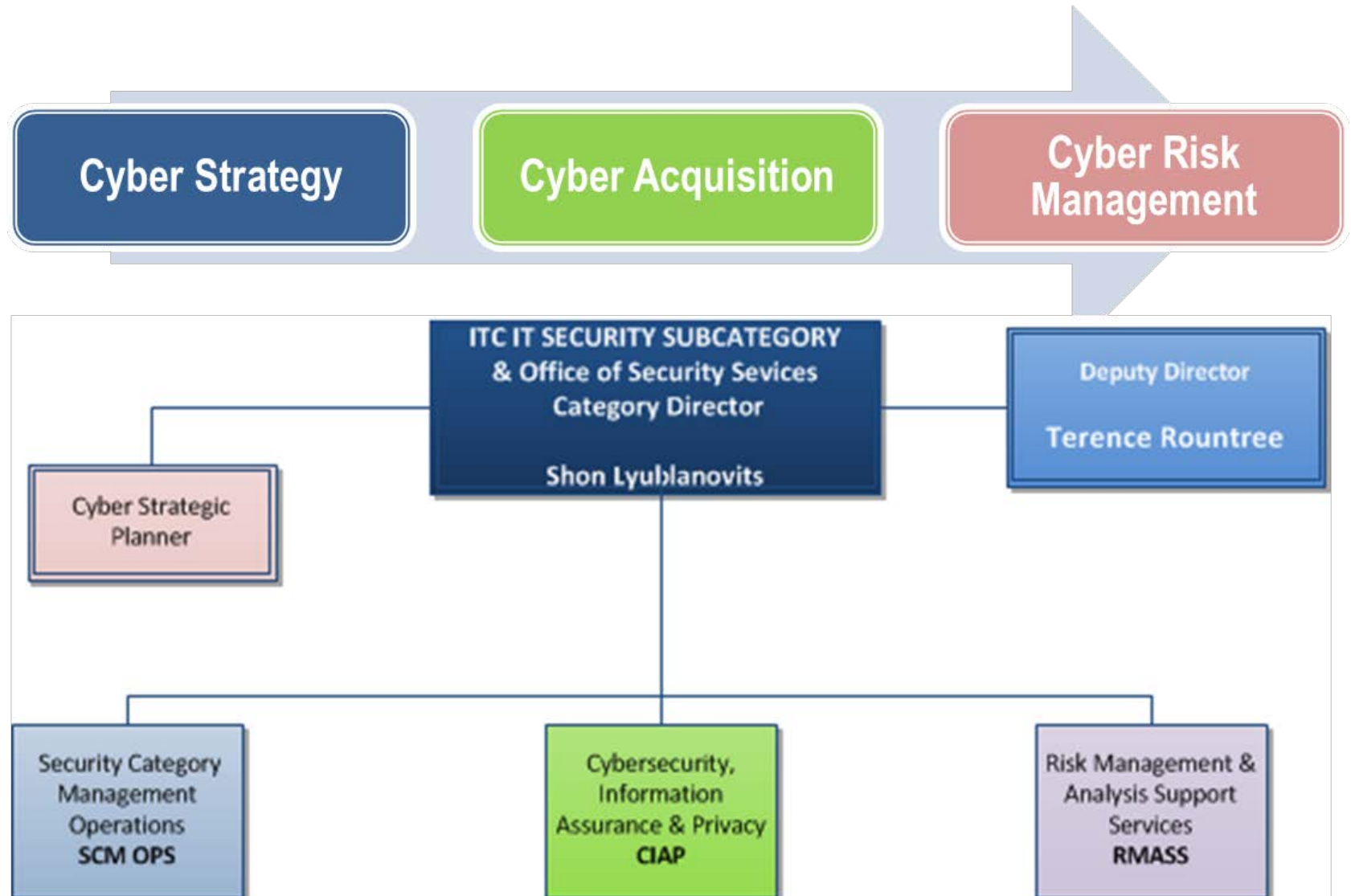
**IT Security Subcategory Manager/
Office of IT Security Services Director**

Mission and Goals

To provide acquisition assurance, expertise, and solutions to guide customers through an ever-changing security landscape; offering them “best value” from a secure marketplace.

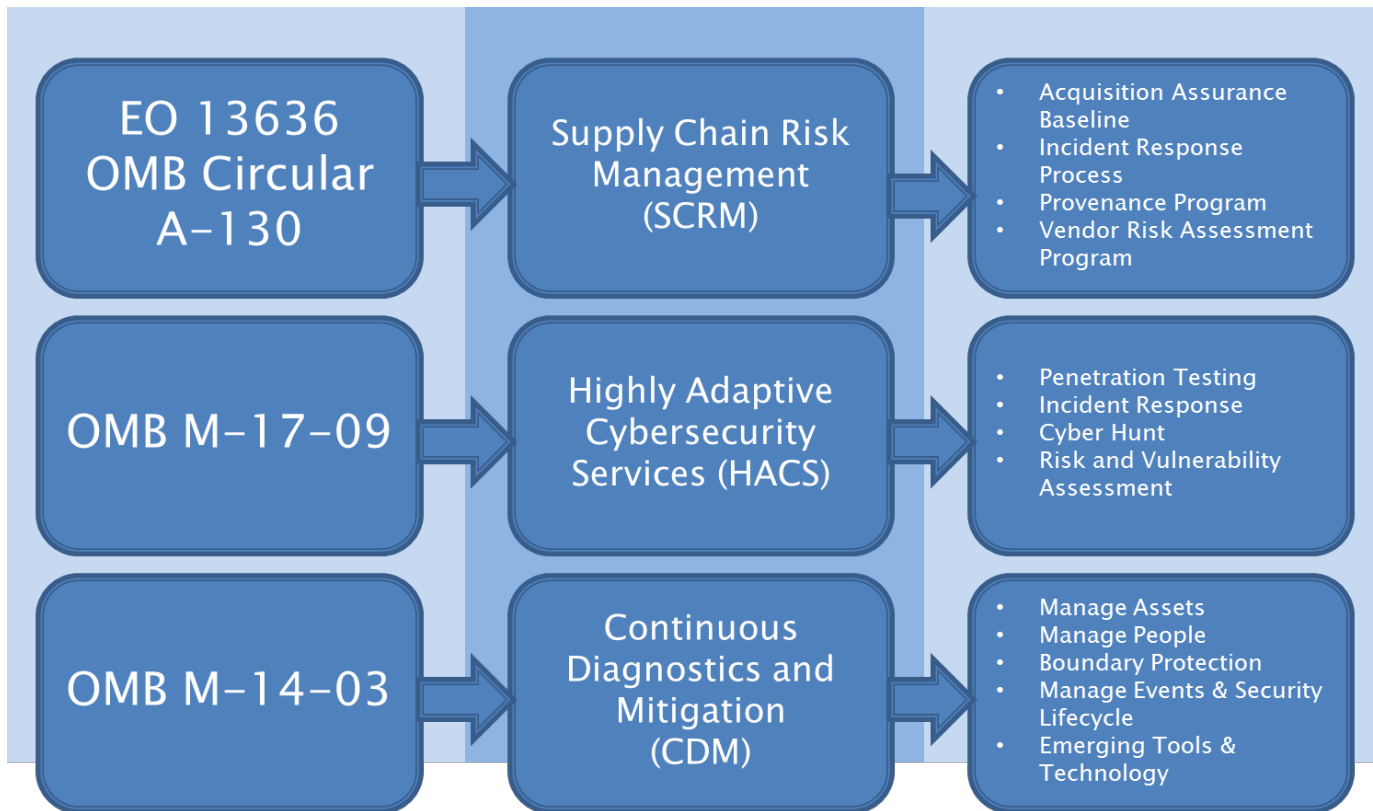


- Trustworthy products and services
- Trusted vendors
- Better contracts



Key Policy Drivers

The IT Security Subcategory helps implement IT policy that enhances the safety and resiliency of our customers' systems and networks.





New Executive Order

The May 11, 2017 Executive Order, “Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,” requires all Federal Agencies and Departments to:

- Implement the NIST Cybersecurity Framework
- Report on cybersecurity risk management efforts
 - Risk mitigation and acceptance
 - Strategic, operational, and budgetary considerations
 - Accepted risk from unmitigated vulnerabilities
- Ensure procurement preferences for IT Shared Services



Improving Cybersecurity and Resilience through Acquisition

GSA and DoD developed recommendations to align Federal cybersecurity risk management and acquisition processes:

- I. Institute baseline cybersecurity requirements as a condition of contract award for appropriate acquisitions
- II. Address cybersecurity in relevant training
- III. Develop common cybersecurity definitions for Federal acquisitions
- IV. Institute a Federal acquisition cyber risk management strategy
- V. Include a requirement to purchase from original equipment manufacturers, their authorized resellers, or other “trusted” sources, whenever available, in appropriate acquisitions
- VI. Increase government accountability for cyber risk management



IT Security Products & Services

GSA offers IT security products and services that help customers improve resilience and protect important information.

- Products and services characterized as “security” are components of one of the other subcategories.
- They protect information and information systems in order to provide confidentiality, integrity, and availability.





Highly Adaptive Cybersecurity Services

Highly Adaptive Cybersecurity Services (HACS) Special Item Number (SINs) on GSA's IT Schedule 70:

- 132-45A: Penetration Testing
- 132-45B: Incident Response
- 132-45C: Cyber Hunt
- 132-45D: Risk and Vulnerability Assessment

Agencies procure services on HACS SINs to:

- Protect systems identified as “High Value Assets”
- Deter the ever-increasing threat of cyber attacks to agencies



Supply Chain Risk Management

Federal Agencies and Departments face hidden risks:

- Grey market and counterfeit products
- Product tampering
- Unlicensed overproduction of authorized components
- Lack of systematic vendor assessments

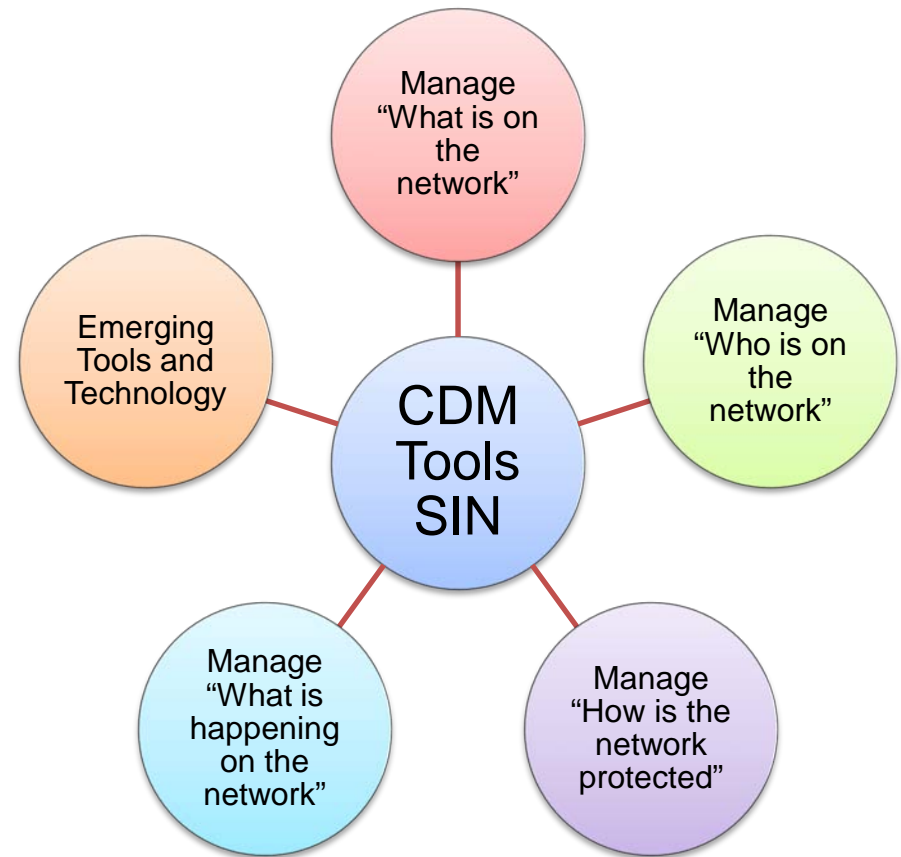
The IT Security Subcategory has addressed Supply Chain Risk Management (SCRM) concerns by:

- Reviewing base contract language
- Establishing a SCRM Incident Response Process
- Conducting a SCRM Provenance Pilot
- Developing a Vendor Risk Assessment Program

Continuous Diagnostics and Mitigation Tools SIN

The 16 Continuous Diagnostics and Mitigation (CDM) Tools and Continuous Monitoring as a Service (CMaaS) Blanket Purchase Agreements (BPAs) are set to expire in August 2018.

- A new CDM Tools SIN is in development; it will provide agencies several CDM capabilities.





Resources and Contact Information

- IT Security Hallway on the [Acquisition Gateway](#)
- For HACS information contact us at: HACS@gsa.gov
- For General IT Security information contact us at:
ITSecurityCM@gsa.gov



Back-up Slides



Additional Policy Drivers

- OMB Memorandum 17-12: Preparing for and Responding to a Breach of Personally Identifiable Information
- NIST SP 800-184: Guide for Cybersecurity Event Recovery, which enables agencies to rapidly recover from incidents when they occur and helps to minimize the impact on the organization and its constituents
- NIST SP 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations
- NIST released NIST Interagency Report (NISTIR) 8062: An Introduction to Privacy Engineering and Risk Management in Federal Systems
- NIST is updating SP 800-63 Suite, expanding the Four (4) Levels of Assurance defined by OMB M-04-04: E-Authentication Guidance for Federal Agencies and mapping them to corresponding authenticator assurance and identity assurance levels



CDM Tools SIN

Subcategory	Capabilities
Manage “What is on the network”	Identify the existence of hardware, software, configuration characteristics, and known security vulnerabilities and include: TFA 1 Hardware Asset Management (HWAM); TFA 2 Software Asset Management (SWAM); TFA 3 Configuration Management (CM); TFA 4 Vulnerability Management (VUL).
Manage “Who is on the network”	Identifies and determines the users or systems with access authorization, authenticated permissions, and granted resource rights and includes: TFA 6 Manage Trust-in-People Granted Access (TRUST); TFA 7 Manage Security Related Behavior (BEHAVE); TFA 8 Manage Credential and Authentication (CRED); TFA 9 Manage Account/Access (PRIV).
Manage “How is the network protected”	Determines the user/system actions and behavior at the network boundaries and within the computing infrastructure and includes: TFA 5 Manage Network Access Controls.
Manage “What is happening on the network”	Prepares for events/incidents, gathers data from appropriate sources, and identifies incidents through analysis of data and includes: The originally identified TFAs of TFA 10 Prepare for Contingencies and Incidents (CP); TFA 11 Respond to Contingencies and Incidents (INC); TFA 14 Manage Audit Information (AUD); TFA 15 Manage Operation Security (OPS); TFA 12 Design and Build in Requirements, Policy, and Planning (POL); TFA 13 Design and Build in Quality (QAL).
Emerging Tools and Technology	Includes CDM cybersecurity tools and technology not in any other subcategory.