U.S. General Services Administration
OFFICE OF INFORMATION TECHNOLOGY CATEGORY

Cyber Supply Chain Risk Management (C-SCRM): The Intersection of Cybersecurity, Supply Chain Management & Acquisition

Thomas Smith
Service Center Director, Office of Supply Chain Risk Management, GSA IT Category

For Government Use Only

Agenda Topics

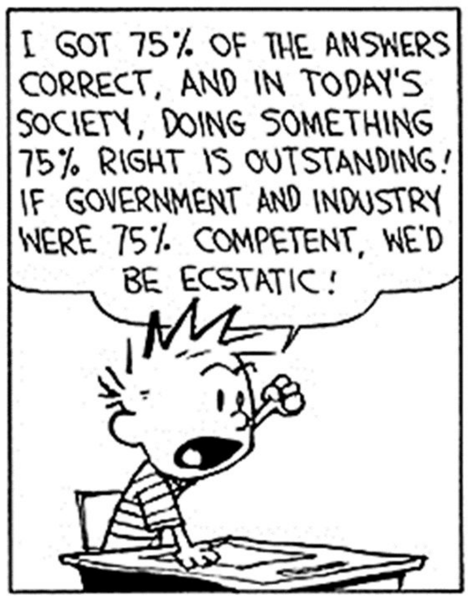
The Challenges

- C-SCRM Risks & Threats: Not Just a Cyber Issue
- Dynamic Regulatory Landscape

Enabling Solutions

- Effective Integration in Technology Procurement
- Supply Chain Risk Illumination Professional Tools & Services (SCRIPTS)

Relational Humor for the Day


I GOT 75% OF THE ANSWERS CORRECT, AND IN TODAY'S SOCIETY, DOING SOMETHING 75% RIGHT IS OUTSTANDING! IF GOVERNMENT AND INDUSTRY WERE 75% COMPETENT, WE'D BE ECSTATIC!

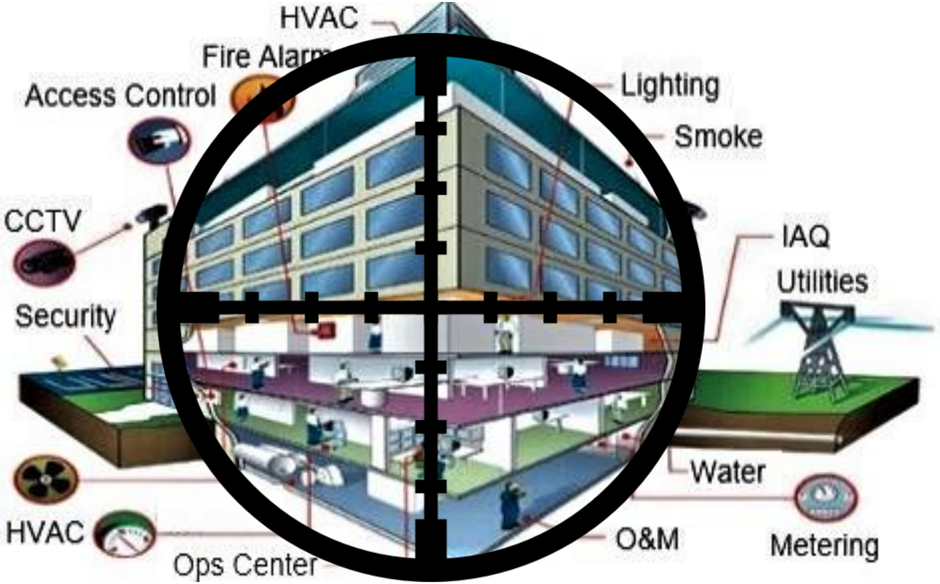
EVERYBODY I KNOW NEEDS WHAT I'M SELLING!
A Swift Kick IN the Butt $1.00
WATTERSON

C-SCRM Risks and Threats

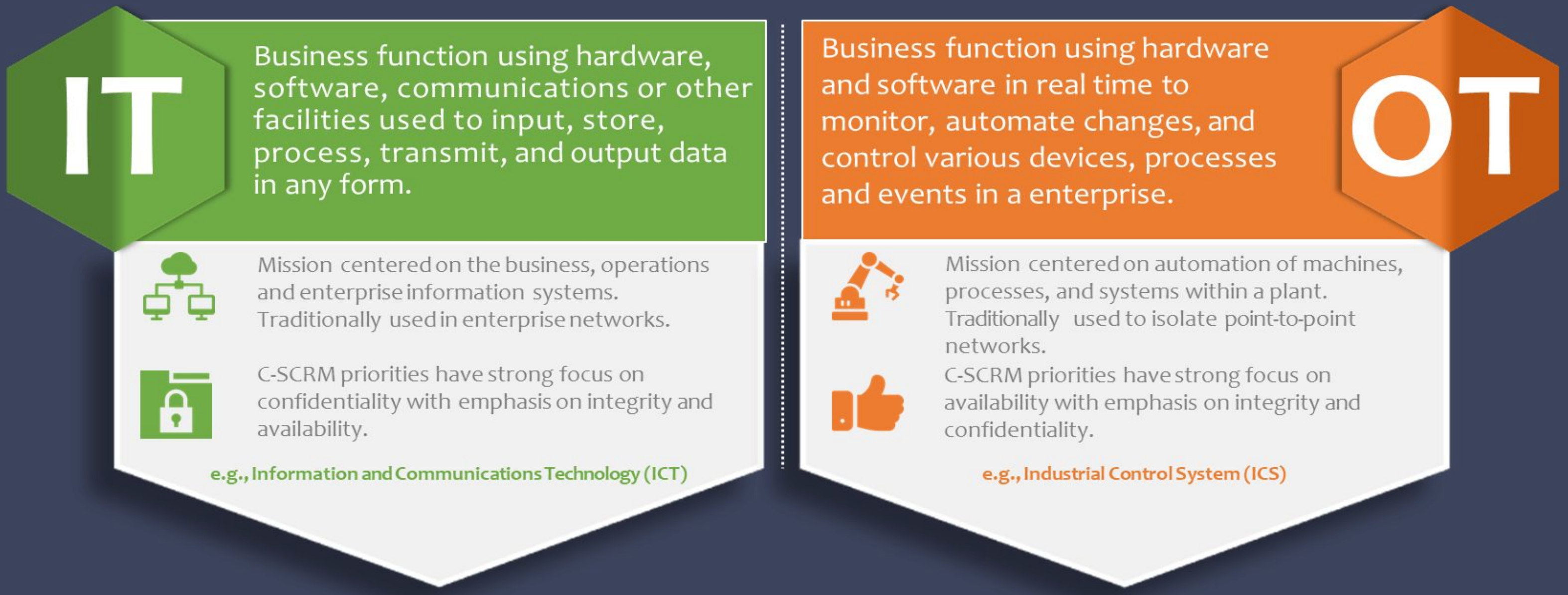
Critical Infrastructure in the Crosshairs

- **GAO Report 21-171, *Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks***
  - **14 / 23 agencies no SCRM practices**

- **[House Select Committee on Strategic Competition Between U.S. and Chinese Communist Party](#) (Feb 2024)**
  - **Volt Typhoon**



Information and Operational Technology (IT/OT)



IT

Business function using hardware, software, communications or other facilities used to input, store, process, transmit, and output data in any form.

Mission centered on the business, operations and enterprise information systems. Traditionally used in enterprise networks.

C-SCRM priorities have strong focus on confidentiality with emphasis on integrity and availability.

e.g., Information and Communications Technology (ICT)

OT

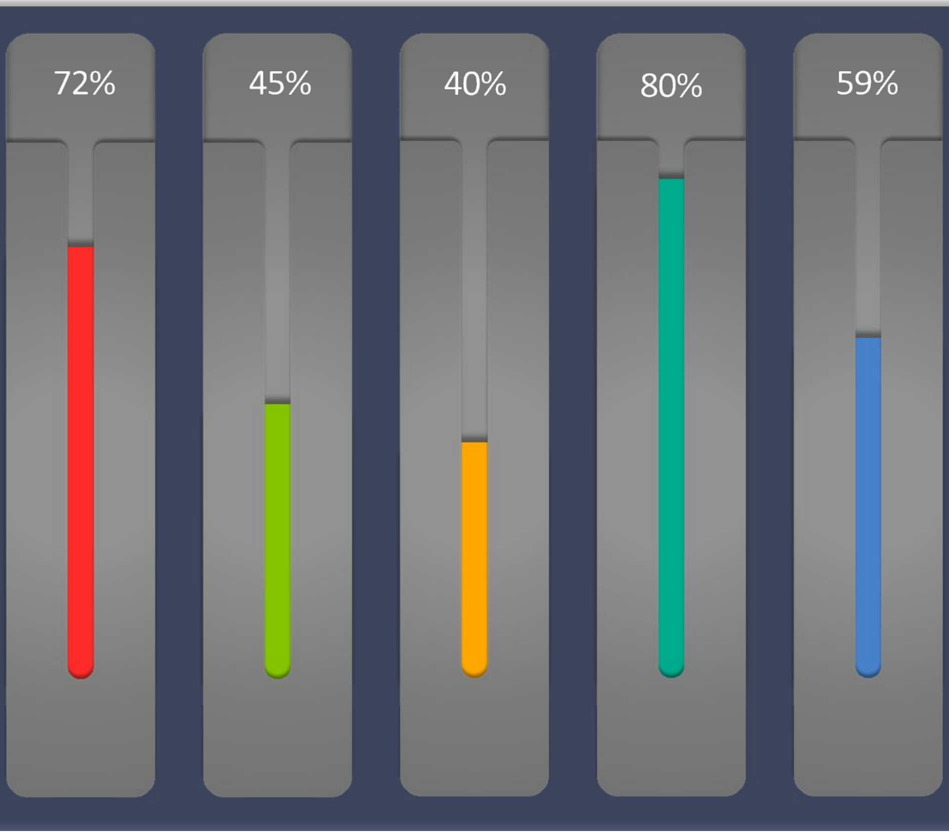
Business function using hardware and software in real time to monitor, automate changes, and control various devices, processes and events in a enterprise.

Mission centered on automation of machines, processes, and systems within a plant. Traditionally used to isolate point-to-point networks.

C-SCRM priorities have strong focus on availability with emphasis on integrity and confidentiality.

e.g., Industrial Control System (ICS)

Once considered separate business domains employing their own unique protection systems, OT/IT functions have begun to converge because of shared cyber supply chain risks.



72% - of companies do not have full visibility into their supply chains

45% - of all cyber breaches were attributed to past partners

40% - of attack campaigns target manufacturing and service sectors

80% - of all information breaches originate in the supply chain

59% - of companies do not have a process for assessing cybersecurity of third-party providers with which they share data or networks

Intersection of Multiple Disciplines

Cybersecurity

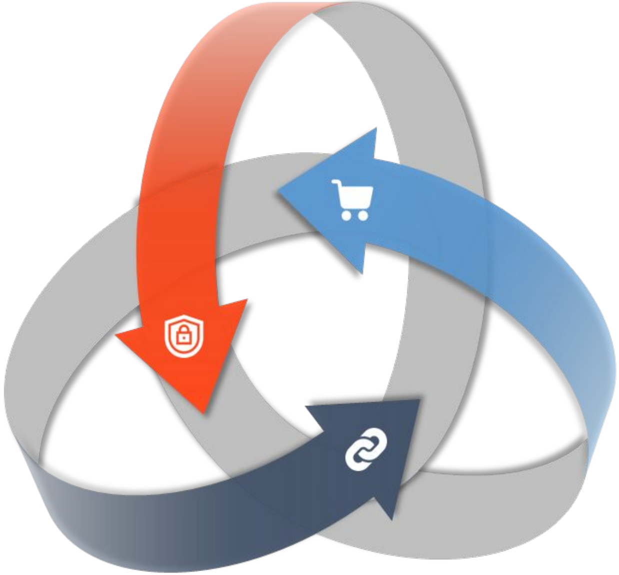
The process of protecting information by preventing, detecting, and responding to attacks.

Supply Chain Risk Management

The process of taking strategic steps to identify, assess, and mitigate the risk in an organization’s end-to-end supply chain.

Acquisitions

The process of acquiring products or services.



How they work together

Preventing compromised components from entering the network will improve cybersecurity and can also increase reliability.

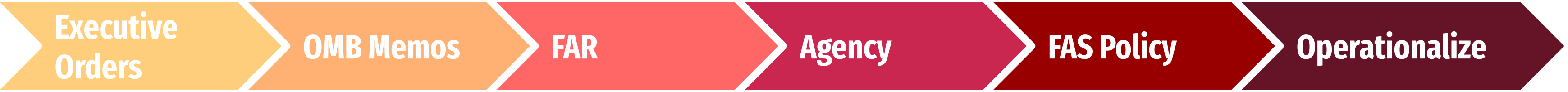
Complexities

Three highly complex, evolving functions that business executives are giving more attention to as the risks facing the supply chain become increasingly prevalent.

How did we get here

Once considered separate business domains employing their own unique protection processes, these three functions have begun to converge because of shared risks.

Dynamic Regulatory Landscape



Executive Orders

Executive Order on America's Supply Chains

Executive Order on Improving the Nation's Cybersecurity

Executive Order on Initiative to Bolster Cybersecurity of U.S. Ports

OMB Memos

M-22-18 Enhancing the Security of the Software Supply Chain through Secure Software Development Practices

M-23-16 Update to Enhancing the Security of the Software Supply Chain

CISA Common Form for Software Attestation & Artifact Repository

FAR

- FASC Exclusion Orders
- Cyber Threat & Incident Reporting
- Cyber Reqs for Fed Info Systems
- Secure Software
- Semiconductor Prohibition

Over the Horizon
-Federal Acq Supply Chain Security Act
- Drones
- Ownership Control & Influence

12 C-SCRM FAR Cases

Agency

Acquisition Workforce Guidance

- Implementation of FASCSA Orders

MV-23-02 - Ensuring Only Approved Software is Acquired and Used at GSA

GSAM - Identify, assess, respond, monitor/control critical ICT risk

FAS Policy

- OIG Audit, Prohibited Items

- Information Sharing w/FASC

- FAS Acquisition Oversight

- Addressing Contract Compliance

- C-SCRM Pre-award

Operationalize

Commercial Supply Chain Illumination Tools

Supply Chain Risk Information Memorandums

Vendor Risk Assessment Reports

SOP on Prohibited Items

SCRM Review Board

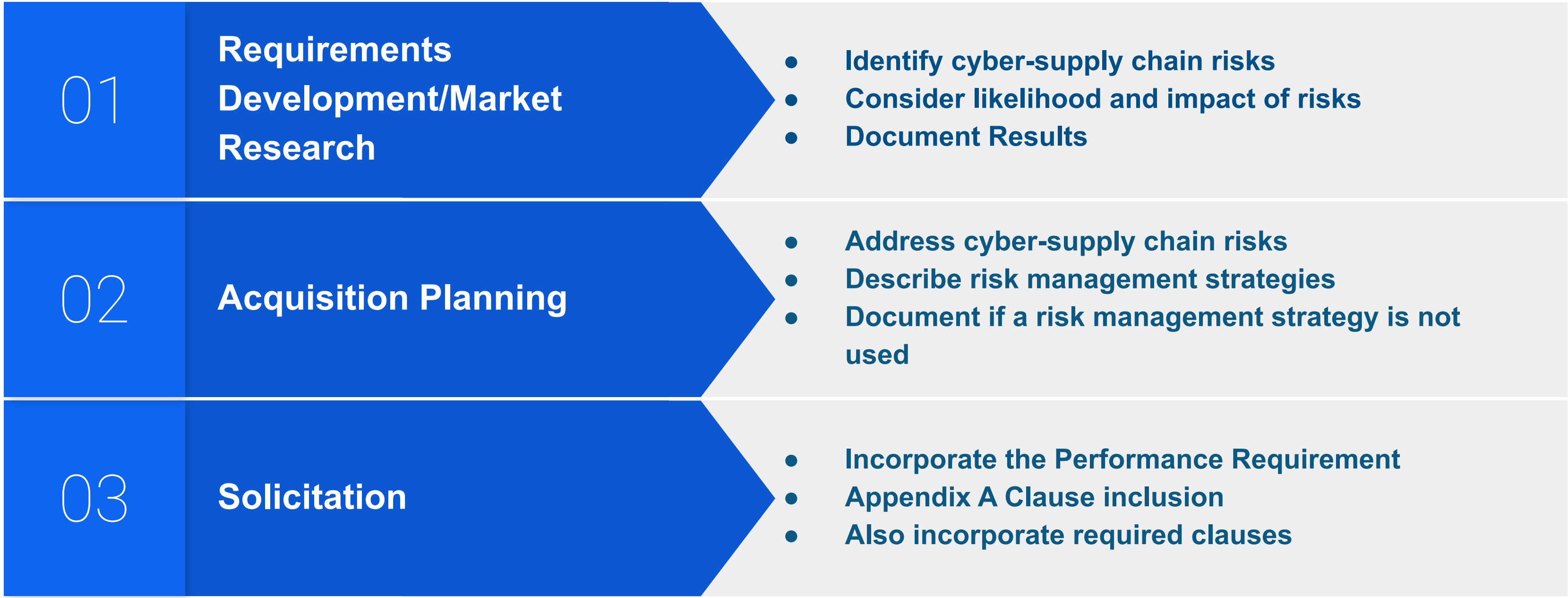
SOP on Suppression

Key Takeaways for Regulatory Deluge

1) Impact to Vendors
   - Cost & Increasing Liability
   - Calculus for remaining in Government market
   - Flow downs to subcontractors, third party
2) Impact to Workforce
   - Guidance & Training
   - Vendor engagement
   - Information Sharing Internally
3) Impact to Systems
   - Modifications
   - Records
4) Interagency & Intra agency Dependencies

Effective Integration in Technology Procurement

Operationalizing C-SCRM in ITC



01 Requirements Development/Market Research

- Identify cyber-supply chain risks
- Consider likelihood and impact of risks
- Document Results

02 Acquisition Planning

- Address cyber-supply chain risks
- Describe risk management strategies
- Document if a risk management strategy is not used

03 Solicitation

- Incorporate the Performance Requirement
- Appendix A Clause inclusion
- Also incorporate required clauses

Operationalizing C-SCRM in ITC

Cyber risk evaluation

- Questionnaire evaluation
  - Evaluate based on responses to minimum required **questions** for product, service, or product/service offering
  - Potential consultation, review & training with offerors
  - Optional risk based

+

C-SCRM Plan evaluation

- Evaluate based on minimum required **controls** for product, service, or product /service offering
- Annual update submission of C-SCRM Plan and questionnaire
- Potential consultation, review & training with offerors

+

Compliance Risks evaluation

- Use VRA or automated tool to ensure no concerns with Section 889, FCC prohibited entities, FASC Exclusion or Removal order

Solicitation, Evaluation, & Award Phase (Pre-award/Pre-performance) Support

Approaches for Applying C-SCRM

Agencies have multiple ways to build C-SCRM throughout the Acquisition Cycle

DIY	Partner
Build specific processes and approaches tailored to their agency	Agencies can look for partnership opportunities across the government that help simplify the C-SCRM process

For any path an agency chooses, GSA has resources to support them on their journey

DIY	Partner
GSA offers Playbooks and Resources developed by Subject Matter Experts Zero Trust Architecture handbook, C-SCRM tool guidebook	GSA offers acquisition vehicles with built in C-SCRM requirements 2GIT IT solutions BPA, Highly Adaptive Cybersecurity Services SIN, and SCRIPTS BPA (future)

Supply Chain Risk Illumination Professional Tools & Services (SCRIPTS) BPA

Description of Need

SCRIPTS

The Office of the Under Secretary of Defense (OUSD), Acquisition and Sustainment (A&S) has a acquisition requirement for a cloud and/or web-based data analytics tool(s) that will perform risk analysis, risk identification, reporting, and continuous monitoring of the supply chain.

The supply chain risk illumination tool(s) will help mitigate the risk of high vulnerability to fraud, abuse, and adversarial exploitation of the supply chain for the DoD and other federal agencies that have shared mission areas with DoD.

Enables foundational support of the 2018 Federal Acquisition Supply Chain Security Act and the Federal Acquisition Security Council (FASC)

SCRIPTS

OFFICE OF THE UNDER SECRETARY OF DEFENSE ACQUISITION AND SUSTAINMENT
DEPARTMENT OF DEFENSE UNITED STATES OF AMERICA

MOU Requiring Agency

DEPARTMENT OF THE AIR FORCE
DEPARTMENT OF THE ARMY
CENTRAL INTELLIGENCE AGENCY
UNITED STATES COAST GUARD
DEPARTMENT OF HEALTH & HUMAN SERVICES USA
DEFENSE INTELLIGENCE AGENCY
DEPARTMENT OF ENERGY
U.S. DEPARTMENT OF HOMELAND SECURITY
DEPARTMENT OF STATE
DEFENSE FINANCE AND ACCOUNTING SERVICE
THE DEPARTMENT OF THE TREASURY
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
UNITED STATES MARINE CORPS
GSA
NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY
NATIONAL RECONNAISSANCE OFFICE
NATIONAL SECURITY AGENCY
DEPARTMENT OF THE NAVY

SCRIPTS

Requirements - FY22 OUSD SCRM Project

- **OUSD A-S SCRM FY22 Project End State Outcomes**
  - Develop supply chain ecosystem and SCRM framework
  - Leverage best practices, pilots, or other efforts already in process
  - Establish DoD SCRM organizational structure, governance & oversight
  - Enable efficiencies, cross-organization collaboration, and consistent data analysis

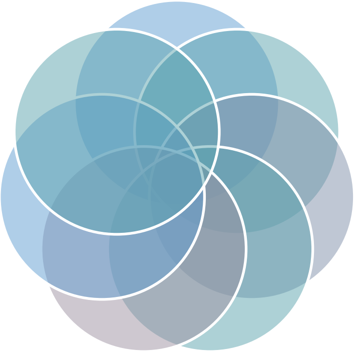
- **Strategic Gap: Resource and maintain enterprise level supply chain ecosystem maps, supplier insight, risk scores, and continuous monitoring to identify systemic risks**

- **Strategic Goal: Create a platform to achieve full spectrum supply chain risk evaluation with common visibility across DoD**

- **Operational Lines of Effort: Acquisition Supply Chain Security, Supply Chain Sustainment, Technology Protection, and Cyber & ICT**

Additional Facilities Collaboration Opportunity

Government Facilities Sector (GFS)



Security experts (cyber-physical)

Law enforcement personnel

Military personnel

Educators & school safety practitioners

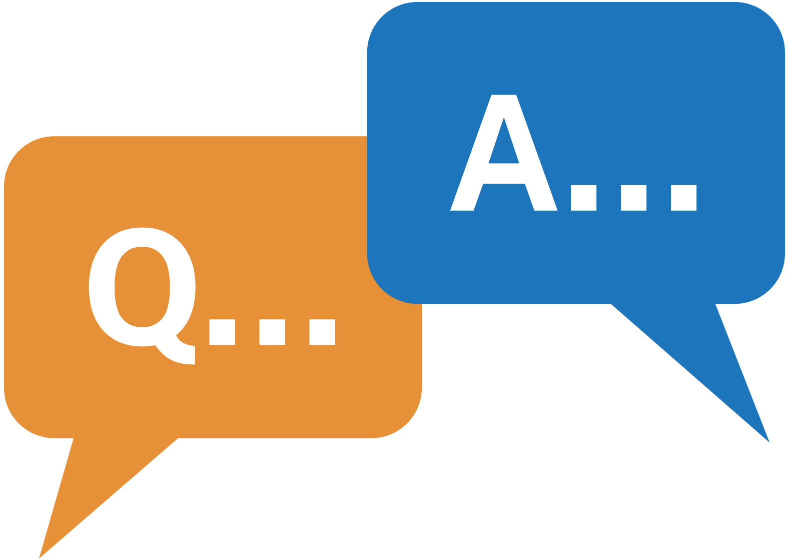
Emergency services practitioners

Elections officials

Health care professionals

The GFS's ultimate goal is to collaborate, coordinate and share information with government stakeholders to help establish and continually enhance the security and resilience posture for government entities—a posture that ensures the safety, security, and protection of employees and visitors to government facilities as well as the facilities assets, systems and resources necessary for delivering mission-oriented services.

Interested in receiving GFS updates? Government staff may email gfs@gsa.gov for consideration.


Q...
A...

THANK YOU

Contact Information:

Email: thomas.smith@gsa.gov

For more information, visit:
gsa.gov/itc