We have several objectives to cover during this session:

- What is the Framework for Improving Critical Infrastructure Cybersecurity?
- Who needs to use the Cybersecurity Framework?
- How do you use the Cybersecurity Framework?
- How has it evolved with the release of Cybersecurity Framework v1.1?
G2 Inc. delivers innovative ideas to solving our nation's critical cybersecurity challenges

- Founded in 2001
- 130+ employees with 2018 revenues in excess of $28M
- Committed to “Turning Ideas into Impact”
- Located in Annapolis Junction, MD
- Mature prime contractor with four active prime contracts
- ManageTheRisk.com
G2 was the primary author of the Cybersecurity Framework through our NIST CSD support contract

- Facilitated and managed eight workshops to collect community feedback
- Interviewed hundreds of cybersecurity subject matter experts from across multiple sectors
- Developed analytic techniques to enable ~15,000 comments to be parsed and individually addressed
- Worked closely with industry partners to develop Cybersecurity Framework Core
- Continues to be involved in the Framework outreach and evolution
Before we begin…

- NIST has MANY Frameworks for helping organizations:
  - Cyber-Physical Systems (CPS) Framework
  - Privacy Engineering Framework
  - Baldridge Excellence Framework
  - Framework for Improving Critical Infrastructure Cybersecurity
    - The Cybersecurity Framework
  - Risk Management Framework (RMF)
  - National Initiative for Cybersecurity Education (NICE) Workforce Framework
Executive Order 13636 established the initial charter for the Cybersecurity Framework

February 12, 2013

“It is the policy of the United States to enhance the security and resilience of the Nation’s critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties”

Executive Order 13636
Executive Order 13636 asked for the creation of a Cybersecurity Framework applicable to all sectors.

- Executive Order
  - Be flexible
  - Be non-prescriptive
  - Leverage existing approaches, standards, and practices
  - Be globally applicable
  - Focus on risk management vs. rote compliance

- Framework for Improving Critical Infrastructure Cybersecurity
  - Referred to as “The Framework” or “Cybersecurity Framework”
  - Version 1.0 issued by NIST on February 12, 2014
  - Version 1.1 released on April 16, 2018
The Framework was developed in partnership among industry, academia, and government.
Executive Order 13636 established the initial charter for the Cybersecurity Framework

December 18, 2014
Amends the National Institute of Standards and Technology Act (15 U.S.C. 272(c)) to say:

“…on an ongoing basis, facilitate and support the development of a voluntary, consensus-based, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to cost-effectively reduce cyber risks to critical infrastructure”

Cybersecurity Enhancement Act of 2014
(P.L. 113-274)
Executive Order 13800 reconfirmed commitment to strengthening cybersecurity for Federal and CI

- EO 13800 - Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
- Risk Management
  - (ii) “…agency head shall use The Framework” and
  - “…provide a risk management report within 90 days containing a description of the “…agency's action plan to implement the Framework.”
- Signed: May 11, 2017
The Framework includes three primary components used to develop a holistic cybersecurity program:

- **Framework Profile**: Aligns industry standards and best practices to the Framework Core in an implementation scenario. Supports prioritization and measurement while factoring in business needs.

- **Framework Core**: Cybersecurity activities and informative references, organized around particular outcomes. Enables communication of cyber risk across an organization.

- **Framework Implementation Tiers**: Describes how cybersecurity risk is managed by an organization and degree the risk management practices exhibit key characteristics.
The Framework Categories provide groupings of cybersecurity outcomes

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDENTIFY</td>
<td>Asset Management</td>
</tr>
<tr>
<td></td>
<td>Business Environment</td>
</tr>
<tr>
<td></td>
<td>Governance</td>
</tr>
<tr>
<td></td>
<td>Risk Assessment</td>
</tr>
<tr>
<td></td>
<td>Risk Management Strategy</td>
</tr>
<tr>
<td></td>
<td>Supply Chain Risk Management</td>
</tr>
<tr>
<td>PROTECT</td>
<td>Identity Management, Authentication and Access Control</td>
</tr>
<tr>
<td></td>
<td>Awareness and Training</td>
</tr>
<tr>
<td></td>
<td>Data Security</td>
</tr>
<tr>
<td></td>
<td>Information Protection Processes and Procedures</td>
</tr>
<tr>
<td></td>
<td>Maintenance</td>
</tr>
<tr>
<td></td>
<td>Protective Technology</td>
</tr>
<tr>
<td>DETECT</td>
<td>Anomalies and Events</td>
</tr>
<tr>
<td></td>
<td>Security Continuous Monitoring</td>
</tr>
<tr>
<td></td>
<td>Detection Processes</td>
</tr>
<tr>
<td>RESPOND</td>
<td>Response Planning</td>
</tr>
<tr>
<td></td>
<td>Communications</td>
</tr>
<tr>
<td></td>
<td>Analysis</td>
</tr>
<tr>
<td></td>
<td>Mitigation</td>
</tr>
<tr>
<td></td>
<td>Improvements</td>
</tr>
<tr>
<td>RECOVER</td>
<td>Recovery Planning</td>
</tr>
<tr>
<td></td>
<td>Improvements</td>
</tr>
<tr>
<td></td>
<td>Communications</td>
</tr>
</tbody>
</table>
Framework subcategories describe expected outcomes

### Framework Core

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify (ID)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset Management (ID:AM)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID:AM-1: Physical devices and systems within the organization are inventoried</td>
<td></td>
<td>• CCS CSC 1</td>
<td>• COBIT 5 BA09.01, BA09.02</td>
</tr>
<tr>
<td>ID:AM-2: Software platforms and applications within the organization are inventoried</td>
<td></td>
<td>• CCS CSC 2</td>
<td>• COBIT 5 BA09.01, BA09.02, BA09.05</td>
</tr>
<tr>
<td>ID:AM-3: Organizational communication and data flows are mapped</td>
<td></td>
<td>• CCS CSC 1</td>
<td>• COBIT 5 DSS05.02</td>
</tr>
<tr>
<td>ID:AM-4: External information systems are catalogued</td>
<td></td>
<td>• COBIT 5 AP002.02</td>
<td>• ISO/IEC 27001:2013 A.11.2.6</td>
</tr>
</tbody>
</table>
Organizations select an Implementation Tier based on their risk threshold
Organizations have applied the Implementation Tiers in different ways and at different levels.
Profiles help organizations align & prioritize cybersecurity activities
Current and Target state Profiles help organizations capture their cybersecurity program

- Current State Profile
  - Present state of the organization’s unique cybersecurity program

- Target State Profile
  - Captures the to-be state for the organization’s cybersecurity program
Cybersecurity Framework v1.1 adds clarity and is fully compatible with v1.0

- Refined for clarity and remains flexible, voluntary, and cost-effective
- Declares applicability for technology
  - Information Technology
  - Operational Technology
  - Physical Systems
  - Internet of Things
- Enhances supply chain guidance
- Clarifies authorization, authentication, and identity proofing
- Cybersecurity Framework Core updates
  - Function 5 → 5
  - Categories 22 → 23
  - Subcategories 98 → 108
The Framework also establishes a common language.
The Framework identifies seven steps for improving or developing a risk informed cybersecurity program:

- Step 1: Prioritize and Scope
- Step 2: Orient
- Step 3: Create a Current Profile
- Step 4: Conduct a Risk Assessment
- Step 5: Create a Target Profile
- Step 6: Determine, Analyze, and Prioritize Gaps
- Step 7: Implement Action Plan
Organizations identify their business and mission objectives to initiate the process

STEP 1: PRIORITIZE AND SCOPE

Mission Goals
Organizational Structure
Priorities
Business Drivers
Regulatory Requirements
Existing Policies
Budget
The orient step aligns the business goals, assets, systems, and regulatory requirements for the program.
A Current Profile captures the organizations policies, procedures, and practices.

### Current Profile

<table>
<thead>
<tr>
<th>Category</th>
<th>Subcategory</th>
<th>Tag Policy</th>
<th>Risk Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Asset Management</td>
<td>Software Inventory and Knowledge within the organization are inventoried</td>
<td>Physical device inventory is inconsistently performed across Division. Some departments have automated systems in place to manage physical device inventories. Many other IT managers maintain a spreadsheet of the assets under their purview. System owners are not required to notify the IT managers if they acquire new systems and the procurement process is not integrated into the ISM. Equipment may be purchased, repurposed, or removed from the department without proper sanitization. Additionally, the Information Security Office uses Quayos to periodically scan department networks and forms its own inventory list, but there are many devices not found using this method.</td>
<td>- Unknown device on network. - No possible to get a complete network baseline. - Creates issues with assigning responsibility as accountability.</td>
</tr>
<tr>
<td>IT Asset Management</td>
<td>Information System Connections with the requirement for Interconnection System Agreements to permit connections outside of the accreditation boundary. Security requirements for the interconnect systems must be documented as well as the nature of the information being shared. The system connections must be continually monitored. Division has the stance of &quot;deny-all, permit-by-exemption.&quot; No policy was provided for testing network/system information security.</td>
<td>- Increased response times to possible that not all stakeholders are made aware of incidents.</td>
<td></td>
</tr>
<tr>
<td>IT Asset Management</td>
<td>Physical Security and System Access Controls</td>
<td>Physical access is inconsistently monitored across Division. Some departments have automated systems in place to manage physical access controls. Many other IT managers maintain physical access control lists for their specific areas. System owners are not required to notify the IT managers if they acquire new systems and the procurement process is not integrated into the ISM. Equipment may be purchased, repurposed, or removed from the department without proper sanitization. Additionally, the Information Security Office uses Quayos to periodically scan department networks and forms its own inventory list, but there are many devices not found using this method.</td>
<td>- Unknown device on network. - No possible to get a complete network baseline. - Creates issues with assigning responsibility as accountability.</td>
</tr>
</tbody>
</table>
A Current Profile captures the organizations policies, procedures, and practices.

### STEP 3: CURRENT PROFILE

<table>
<thead>
<tr>
<th>ID.AM-1</th>
<th>ID.AM-2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Org Policy</strong></td>
<td><strong>Org Practices</strong></td>
</tr>
<tr>
<td>POL-CM Configuration Management v2.1, section Information System Component Inventory (CM-8), states that information systems must be inventoried and relevant ownership information must be kept. It states what type of information must be documented, and when the inventory should be updated. It also states the need for an automated detection system which can identify unauthorized hardware, software, and firmware.</td>
<td>Physical device inventorying is inconsistently performed across Division. Some departments have automated systems in place to manage physical device inventories. Many other IT managers maintain a spreadsheet of the assets under their purview. System owners are not required to notify the IT managers if they acquire new systems and the procurement process is not integrated into the ISO. Equipment may be purchased, repurposed, or removed from the department without proper sanitation. Additionally, the Information Security Office uses Qualys to periodically scan department networks and forms its own inventory list, but there are many devices not found using this method. Division is in the process of implementing an automated mechanism to monitor Division's networks for new devices; however it is not fully implemented at this time.</td>
</tr>
<tr>
<td></td>
<td>Software device inventorying is not performed in a consistent manner across Division departments. No department interviewed appears to have any form of software inventory system other than basic patch management.</td>
</tr>
</tbody>
</table>
A security risk assessment identifies those risks the organization must address.
A risk register is a common way to define the likelihood and impact of threats acting on vulnerabilities.

<table>
<thead>
<tr>
<th>Subcategory</th>
<th>ID.AM-1: Physical devices and systems within the organization are inventoried, PR.DS-5: Protections against data leaks are implemented</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Threat Source</strong></td>
<td><strong>Vulnerability Summary</strong></td>
</tr>
<tr>
<td>Insider (accidental), Insider (adversarial), Outsider (adversarial)</td>
<td>Physical devices are not consistently inventoried. Software and data on most systems is not tracked or associated with physical devices. Most systems are encrypted, but it is not tracked which are or are not.</td>
</tr>
<tr>
<td><strong>Risk Event</strong></td>
<td>If a device is lost, personnel will not understand what data has been lost or exposed.</td>
</tr>
<tr>
<td><strong>Likelihood</strong></td>
<td><strong>Impact</strong></td>
</tr>
<tr>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td><strong>Risk Level</strong></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td></td>
</tr>
</tbody>
</table>
Incorporating regulatory requirements with risks establishes a robust cybersecurity program.
A Target State Profile captures the policies and practices required to mitigate risks within acceptable thresholds.
Where you start is less important than the accuracy of the information recorded.
Next organization assess their current and target cybersecurity programs to identify gaps.

**STEP 6: DETERMINE, ANALYZE, AND PRIORITIZE GAPS**
The final step is to implement and monitor an action plan to close identified gaps.

**STEP 7: IMPLEMENT ACTION PLAN**
Two unique Cybersecurity Framework implementations that added value
The University of Chicago used the Cybersecurity Framework to align goals.
Intel used the Framework to identify deltas in their cybersecurity program.

![Image: Heat Map]

**Figure 1.** A heat map resulting from charting individual and group scores and their comparisons. Note: The scores given are examples and not the actual scores.
Questions?

Tom Conkle
Cybersecurity Engineer
Tom.Conkle@G2-inc.com
(443) 292-6679

Visit us at: ManageTheRisk.com