Government-Industry Collaboration:

7 Steps for Resiliency in Critical Infrastructure Protection

L. Laile Di Silvestro
Senior Strategist
Worldwide Public Sector
Microsoft

Legal Foundation and Regulatory Environment

National Strategy

Industry Partnership

Culture of Security

Incident Response, Watch and Warning, and Recovery

Government – Industry Collaboration

7 Steps for Resiliency in Critical Infrastructure Protection

Government, infrastructure owners/operators, and IT vendors can collaboratively pursue these core enablers of resiliency and infrastructure security

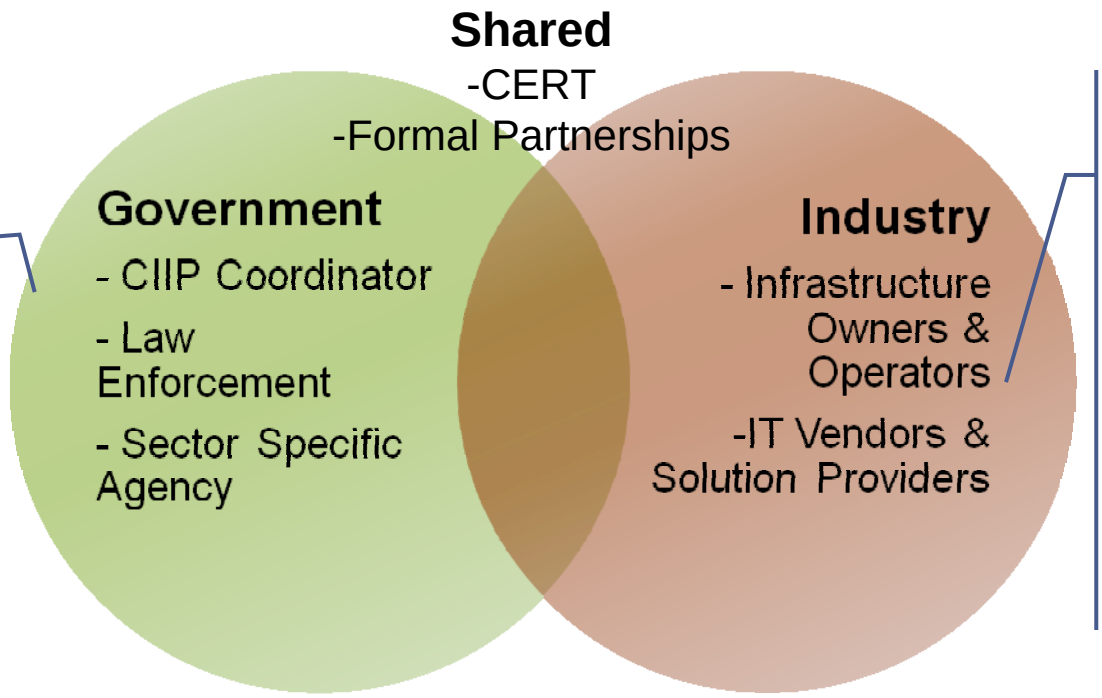
1. **Define Goals and Roles**
2. **Create Public-Private Partnerships**
3. **Identify and Prioritize Critical Functions**
4. **Continuously Assess and Manage Risks**
5. **Establish and Exercise Emergency plans**
6. **Build Security/Resiliency into Operations**
7. **Update and Innovate Technology/Processes**

1. CIP Goals & Roles

Establishing Clear Goals and Roles is Central to Success

Policy Element	Sample Policy Statement
Public-Private Implementation	Implementing the National CIIP framework includes government entities as well as voluntary public-private partnerships involving corporate and nongovernmental organizations.

•Leads CIIP activities
•Prevents, investigates and prosecutes cybercrime
•Coordinates national risk management for all sectors



•Prioritize assets, analyze levels of impact, define acceptable risk, implement control solutions
•Provide products & services critical to CI IT infrastructure

2. Create Public-Private Partnerships

Collaboration is key to protecting critical infrastructure

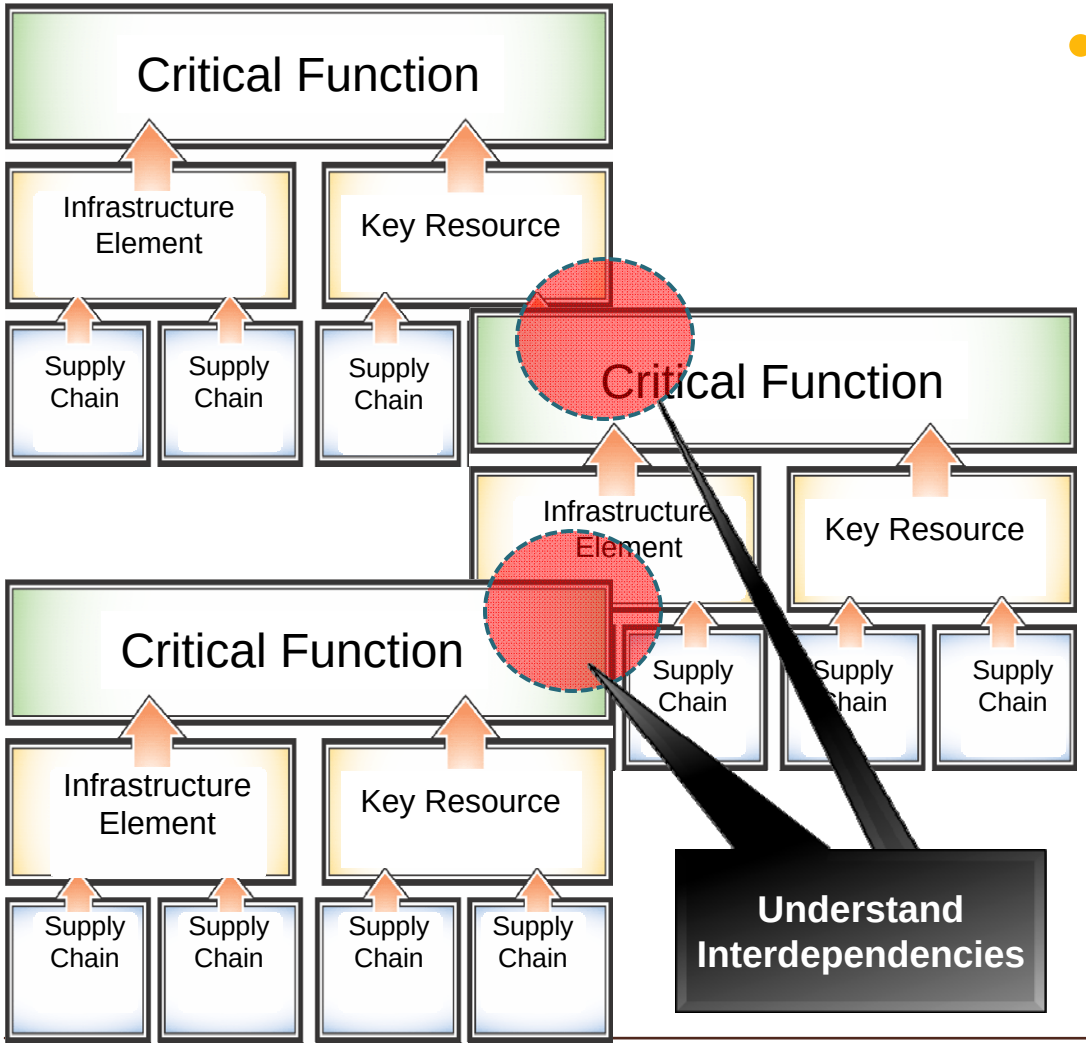
- Voluntary public-private partnerships
  - Promote trusted relationships needed for information sharing and collaborating on difficult problems
  - Leverage the unique skills of government and private sector organizations
  - Provide the flexibility needed to collaboratively address today's dynamic threat environment

BEST PRACTICES

1. Establish formal agreement to set expectations
2. Agree on level of industry contribution before incidents occur
3. Leverage formal, structure programs

3. Identify and Prioritize Critical Functions

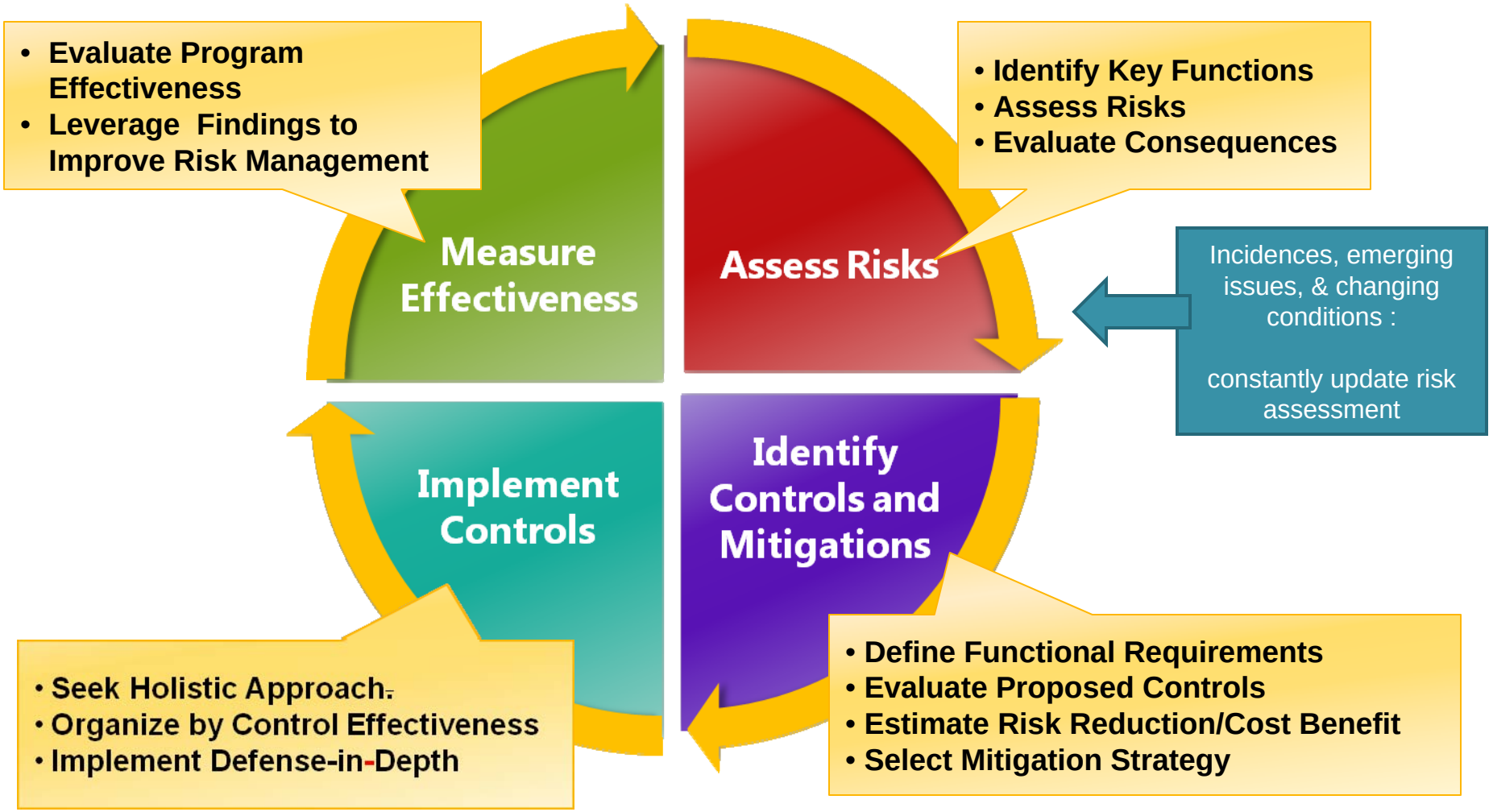
Collaborate to understand Interdependencies



- Establish an open dialogue to understand the critical functions, infrastructure elements, and key resources necessary for:
  - delivering essential services,
  - maintaining the orderly operations of the economy, and
  - helping to ensure public safety.

4. Continuously Assess and Manage Risks

Protection is the Continuous Application of Risk Management



5. Establish and Exercise Emergency plans

Improve Operational Coordination

- Public- and private-sector organizations alike can benefit from developing joint plans for managing emergencies, including recovering critical functions in the event of significant incidents, including but not limited to:
  - natural disasters
  - terrorist attacks
  - technological failures
  - accidents.
- Emergency response plans can mitigate damage and promote resiliency.
- Effective emergency response plans are generally short and highly actionable so they can be readily tested, evaluated, and implemented.
- Testing and exercising emergency response plans promotes trust, understanding, and greater operational coordination among public- and private-sector organizations.
- Exercises also provide an important opportunity to identify new risk factors that can be addressed in response plans or controlled through regular risk management functions.

Security Cooperation Program

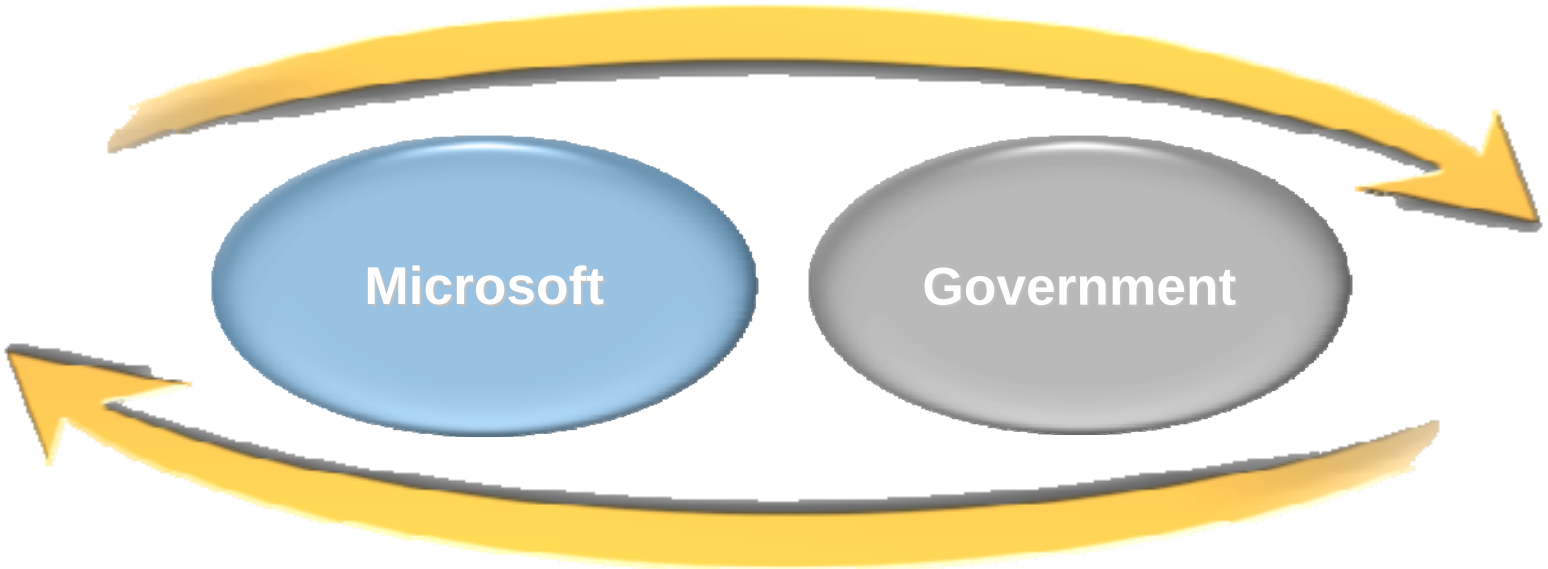
Overview

- A worldwide program providing a structured way for governments and governmental organizations responsible for computer incident response, protection of critical infrastructure, and computing safety to collaborate with Microsoft in the area of IT security
- Includes incident response, information exchange, and public outreach components

Benefits

- Public/private partnership in incident response and information exchange can help decrease risk to national security, economic strength, and social welfare from attacks on the country's IT infrastructure.
- Microsoft provides a 24/7 hotline for SCP participants, and works with participants to define a process for disseminating information in the event of a critical incident or emergency.

SCP - Information Exchange



To Governments:

- Alerts and advisories
- Security metrics
- Attack indicators
- Mitigations

To Microsoft:

- Security metrics
- Incident details
- Product feedback

6. Build Security & Resiliency into Infrastructure

Security is a continuous process

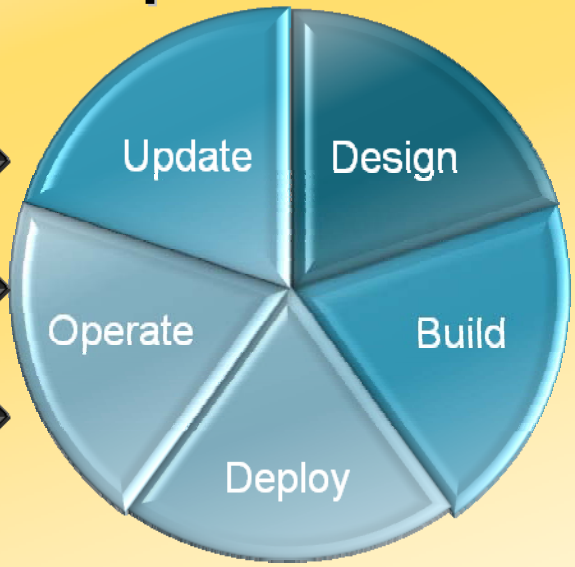
Building security and resiliency into infrastructure operations

Critical Functions
(Global, National, Local)

Infrastructure Operations

Security Controls

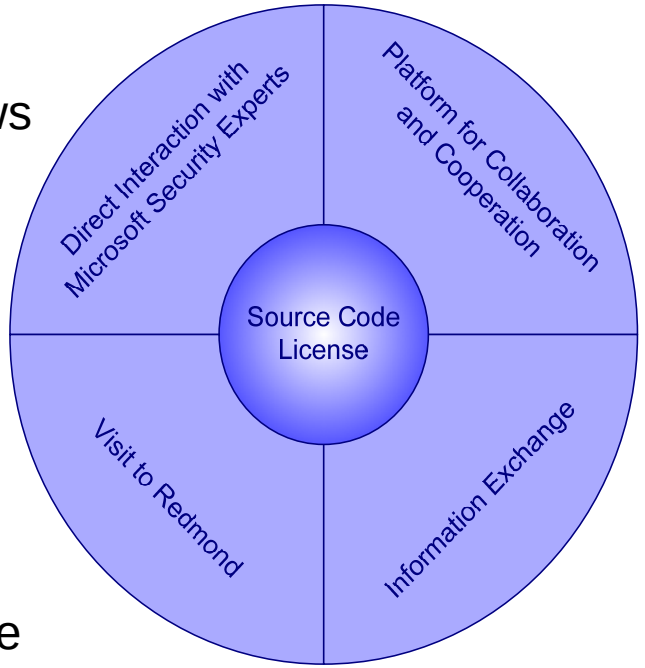
- **Management**
- **Technical**
- **Operational**



Fosters increased security and resiliency for the critical functions that support safety, security and commerce at all levels

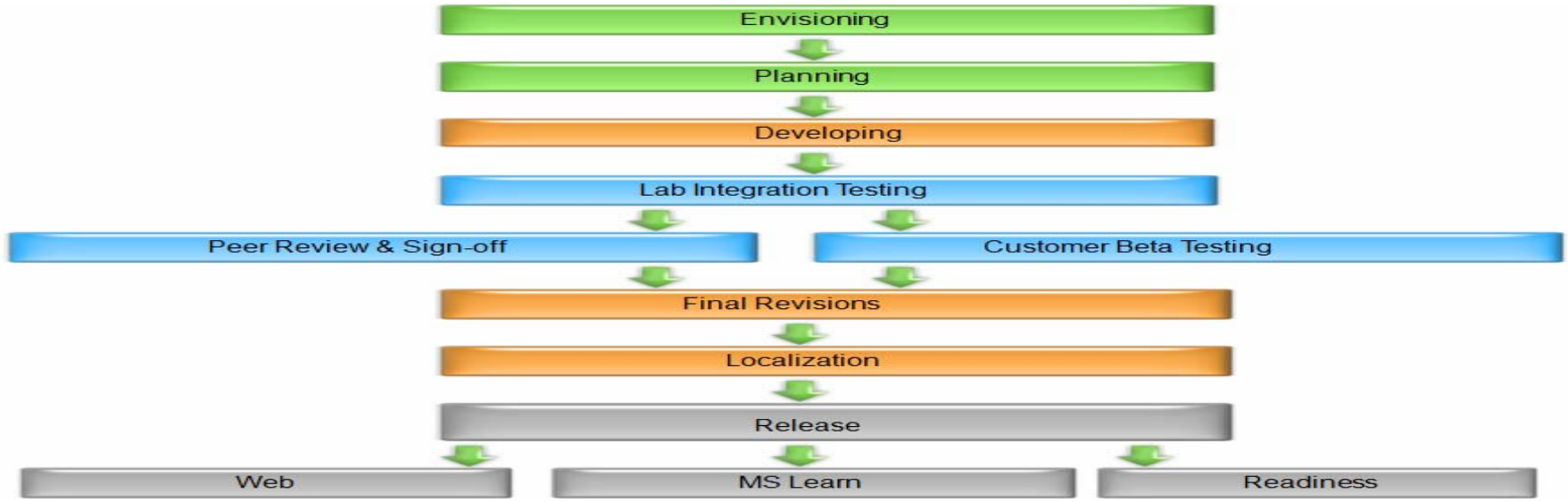
Government Security Program

- Access to source code of Windows Vista, Windows 2000, Windows XP, Windows Server 2003, Windows CE, and Office 2003 / 2007
- Access to Microsoft security and other technical experts
- Access to security and source code training
- Access to documentation relating to security
- Access to information about how Microsoft implements security on its own networks
- Access to authoritative, prescriptive and supportable security guidance for core operating systems and products.



Systems Hardening Program

- Provide early input on security guidance.
- Participate in co-development and testing of prescriptive security guidance.
- Improve products and prescriptive guidance through collaborative feedback and testing.
- Balance security with mutually agreed authoritative security guidance supported by Microsoft.
- Security Guide customization.



7. Update and Innovate Technology/Processes

Mitigate threats by keeping technology current and practices innovative

- Cyber threats are constantly evolving
- Policymakers, enterprise owners, and infrastructure operators can prepare for changes in the threat landscape by:
  - Monitoring trends
  - Keeping systems updated
  - Maintaining the latest versions of software that have been built for the current threat environment

Summary: Government-Industry
Collaboration Opportunity Areas

Skills Training

- Contribute to public sector capacity building efforts & share tools/technologies

Risk / Threat Assessment

- Collaborate on methodologies and tools

Technology Updates

- Technologies, best practices & prescriptive guidance
- Enable collaboration across "community of practice"

Incident Response Role Definition

- Define the Industry contribution before apparent need

Questions?