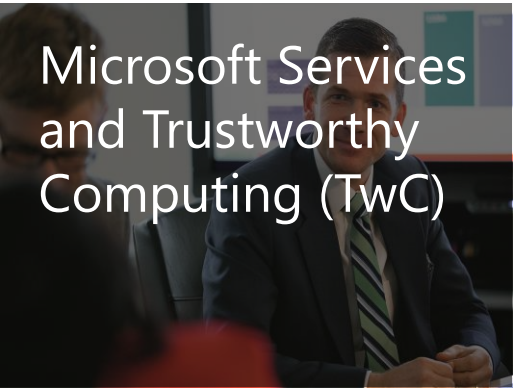
Partnership Perspectives…\Building Blocks for CYBERSECURITY

Vernon L. Lee, MSc., CISSP
Microsoft Services
Federal Civilian CTO



Microsoft Services

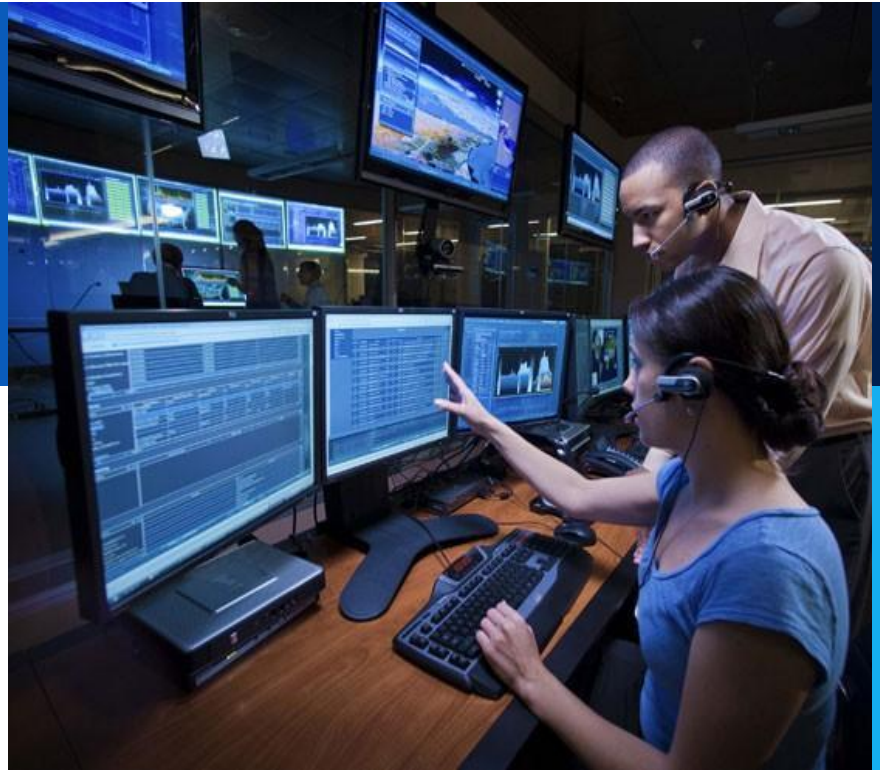
Microsoft Services is a diverse team of architects, engineers, consultants, and support professionals. Our more than 20,000 people live and work around the world, serving customers in 191 countries and helping them in 46 different languages.

Our Services Mission is to lead and serve our customers and partners as they realize their full potential through software and services. To achieve our mission, we hold ourselves accountable to the four goals of CPE, People, Market Share, and Operational Excellence and manage our organization through five business areas: Enterprise Strategy, Consulting Services, Premier Support, Broad Customer Service and Support, and Partner Enablement.

Trustworthy Computing (TwC)

The security of our customers' computers and networks is a top priority. We are committed to building software and services that help protect our customers and the industry. Our approach to security includes both technological and social aspects, and we strive to ensure that information and data are safe and confidential. Drawing on industry best practices, we make investments to increase the security of our technologies and to provide guidance and training to help minimize the impact of malicious software.

Work Completed in Partnership with NIST and NCCoE



Microsoft embraced NIST's standards and guidance on PIV:

- OCD of the Microsoft CA for PIV
- Partnered with Intercede, Gemalto, CyberTrust to deploy PIV for the Executive Office of the President

Additionally, we provided resources to work with NIST & NCCoE on the following:

- USGCB\FDCC GPOs
- HIPAA security settings and GPOs
- NIST PIV test cards and Hyper-V test lab
- UEFI - secure boot configuration and WinPE based BIOS updates

Partnership Perspective

We expect that partnership will result in better CYBERSECURITY guidance in three ways:

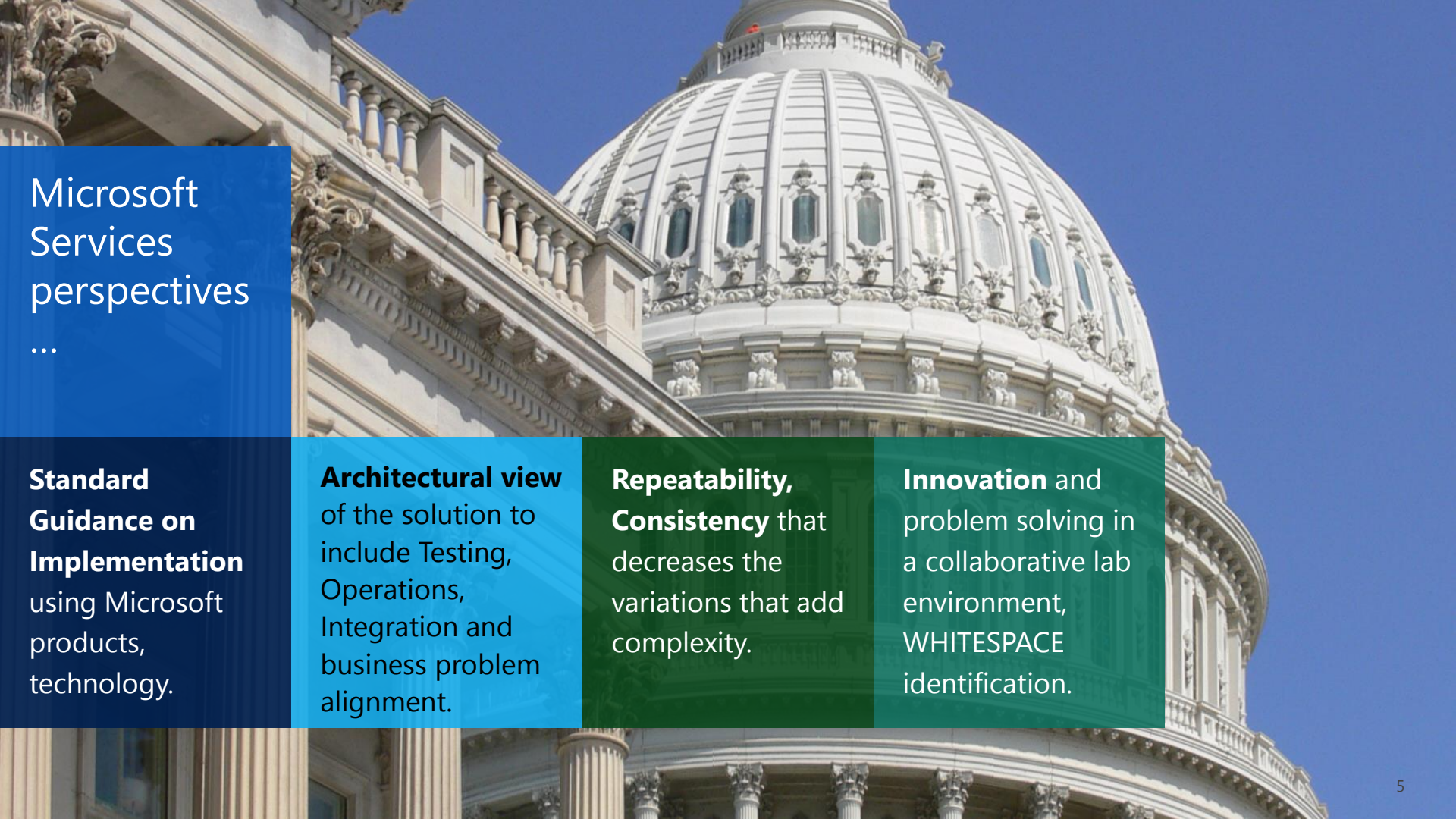
- **Simplification**: security guidance needs to either be simple enough for non-experts to implement or it should be automated/built-in to the systems from the beginning.
- **Acceleration of adoption**: the partnership can help rapidly develop security solutions in emerging areas such as eHealth, internet of things, etc. such that we don't have to wait for a security crisis to address the issues.
- **Securing the seams**: many potential security issues appear at the intersection of systems or components. The NCCoE model lets us look at the security of the entire system, freeing implementers from having to wrestle with potentially conflicting requirements or guidance.

TwC established in 2002 to deliver secure, private, and reliable computing experiences

Opportunities for Microsoft and other organizations to collaborate on key CYBERSECURITY challenges

Cannot be solved by ANY one organization, collaborative nature allows work in real world environments

Microsoft Services provides a local resourcing model of technical SMEs to engage as Guest Researchers at the NCCoE…



Microsoft Services perspectives …

Standard Guidance on Implementation using Microsoft products, technology.

Architectural view of the solution to include Testing, Operations, Integration and business problem alignment.

Repeatability, Consistency that decreases the variations that add complexity.

Innovation and problem solving in a collaborative lab environment, WHITESPACE identification.

Microsoft CYBERSECURITY

Proven success with a track record in Commercial and Government…

- Key player on Policy and Operational sides
- Organization must move to a Risk based security posture
- Range of options: secure coding to real-time monitoring

Response & Investigation

- **IR – Incident Response**
- **PADS – Persistent Adversary Detection Service (proactive incident response)**

Recovery & Mitigation

- **SERA – System Error Reporting & Analysis**
- **MTDS – MSFT Threat Detection Service**

Architecture & Advisory

- **CSA – Cyber Security Architect; assessment (includes people, process, technology, road mapping)**
- **AD – improve AD posture through hardening**
- **Cyber Assessment & Planning Engagement**
- **IdM – everything from provisioning and de-provisioning of users who is on your system) to administrative privilege**

Services, Software and Products available and provided for the lab…

MSDN or TechNet Windows Server & Clients, Forefront Identity Management Server, Systems Center Operations and Configuration Manager, + all Microsoft software

Microsoft Consulting Services Architects, Microsoft Health IT consultants, other SMEs

Access to **O365** trials and **Azure PaaS** & **IaaS** developer instances, and Windows Azure Active Directory

Microsoft **Surface Pro** and **Windows Phone** devices

Contact
Vernon L. Lee
Civilian CTO

(407) 489-6738
Vernon.Lee@Microsoft.com