Intelligence & National Security Forum

Achieving Resilience in Our Nation's Mission Critical Architectures with Real-Time Situational Awareness

May 11, 2018

This presentation is unclassified in its entirety

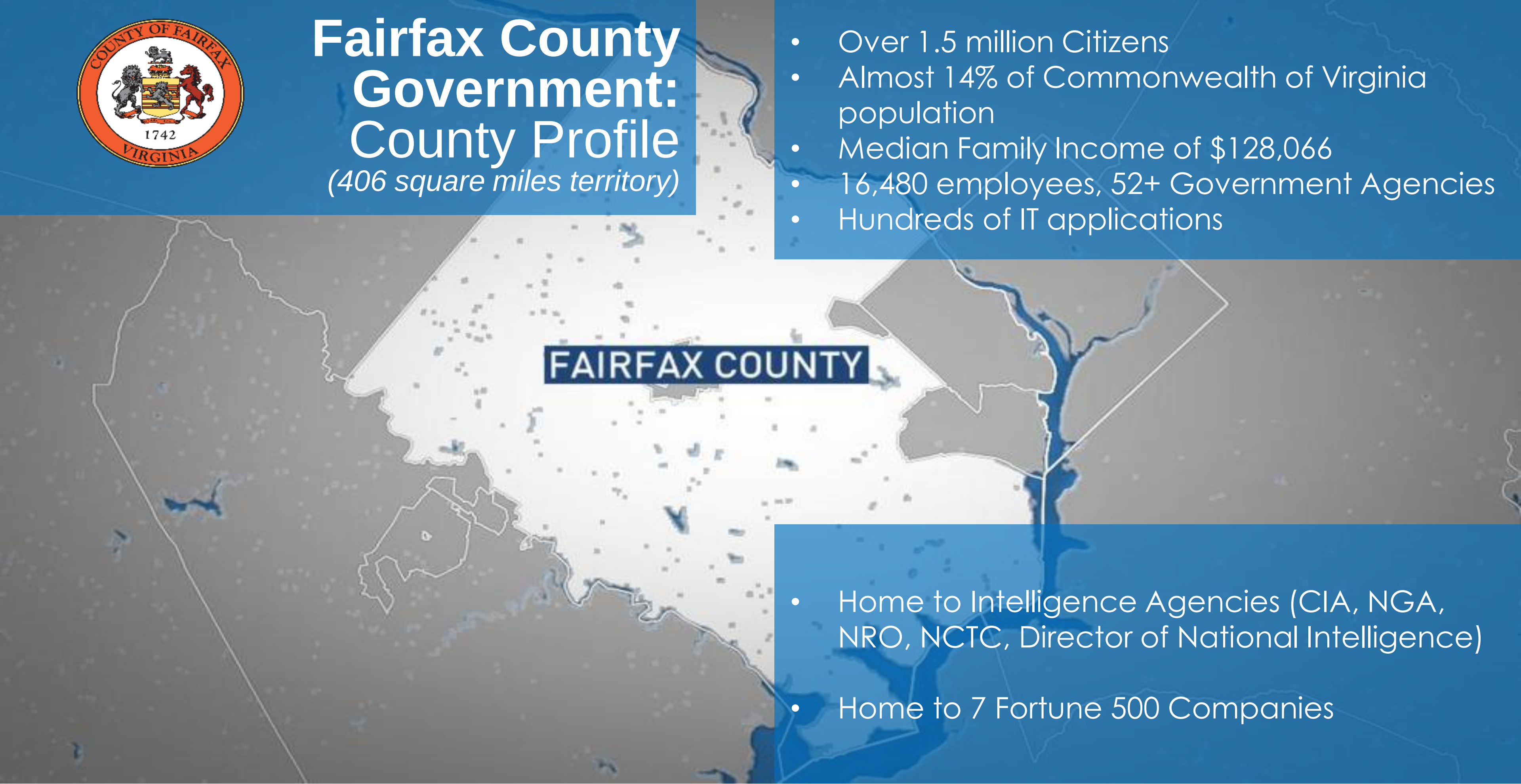
A chief information security officer (CISO) is the senior-level executive within an organization responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected. The CISO directs staff in identifying, developing, implementing, and maintaining processes across the enterprise to reduce information and IT and OT risks. They respond to incidents, establish appropriate standards and controls, manage security technologies, and direct the establishment and implementation of policies and procedures

Fairfax County Government
CISO: Michael Dent

Fairfax County Government: County Profile

(406 square miles territory)

- Over 1.5 million Citizens
- Almost 14% of Commonwealth of Virginia population
- Median Family Income of $128,066
- 16,480 employees, 52+ Government Agencies
- Hundreds of IT applications



- Home to Intelligence Agencies (CIA, NGA, NRO, NCTC, Director of National Intelligence)
- Home to 7 Fortune 500 Companies

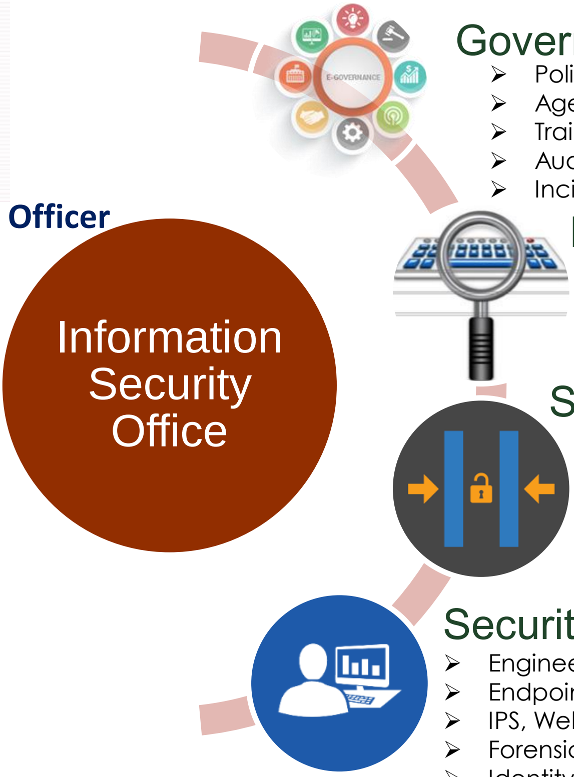
➢ Cyber Security Program

Defense in Depth

Our Vision and Mission: Protect Citizen's Data, Develop & Enforce Security Policies and use best of breed technology

Compliance Officer

CISO



Information Security Office

Governance & Awareness

- Policy & Standards Development
- Agency Consultation & Coordination
- Training Development
- Audit, Assessment, Compliance, Auditing, Reporting
- Incident Response

Monitoring & Investigations

- Ediscovery, Malicious Code, Breaches
- Policy Violations, Misuse, Personnel Issues
- Internal Audit

Security Architecture Design

- Application & Infrastructure Design
- HIPAA Security Rule, PCI-DSS
- Industry Best Practices
- Architectural Review Board
- Security In-Depth Approach

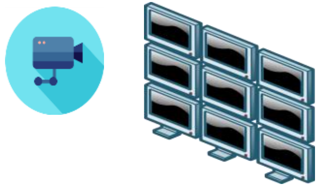
Security Operations

- Engineering & Administration, Endpoint Protection,
- Endpoint management, Patches & Updates, Firewalls
- IPS, Web Filters, Malware Detection, SIEM & Log Analysis
- Forensics, Mobile Device Management, DLP
- Identity Management, Access Control, Remote Access
- Cloud Security

NEW CONNECTED LANDSCAPE

Consumer & Home

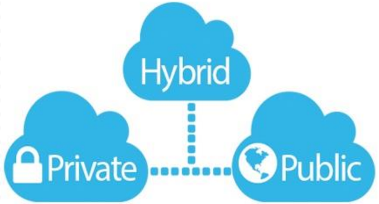
Smart Cities



Security & Surveillance

Healthcare

Public Safety



Transportation

Retail & ECommerce

Critical Infrastructure

Government

Cyber Threats

Connected Landscape

- Smart Cities
- Healthcare
- Public Safety
- Transportation
- Critical Infrastructure
- Security & Surveillance
- Consumer & Home

Start of Modern Cyber Attacks

- Sophisticated, Government Targets
- Malware, Spyware, BOTNets, DDOS, Ransomware
- Email (Spam, Phishing, Spear Phishing)
- Public and Private sector breache
- Application-based threats
- Identity thefts

New Threat Landscape

- **Critical Infrastructure**
- CLOUD Computing
- Mobile Computing
- Internet of Things (iOT)
- Transportation, Healthcare, Smartcity, Retail, banking, industrial, etc...

Threats

Security Ecosystem (Our Security Approach, Defense In-depth)

Defense

In-depth

Endpoint Security

- Machine learning Artificial Intelligence endpoint protection

- Endpoint asset inventory, patching

NextGen Firewall

Internet Perimeter and Access
Application Visibility & Control
Advanced Threat Detection
SSL Decryption

Cloud Security

Cloud security brokers, Cloud app detection, analytics, Secure moving Data

SIEM & CI Real-time Data Analytic Tools

- Real-time logging
- Correlation
- Alerting & Notification
- Visibility & Reporting

Email Security

IdentifyFraud & Abuse
Spear-Phishing Protection
Alert & Blocking of Email threats

Network Architecture

Network Design & Segmentation
Traffic Enforcement points
Perimeter Security, Virtualization

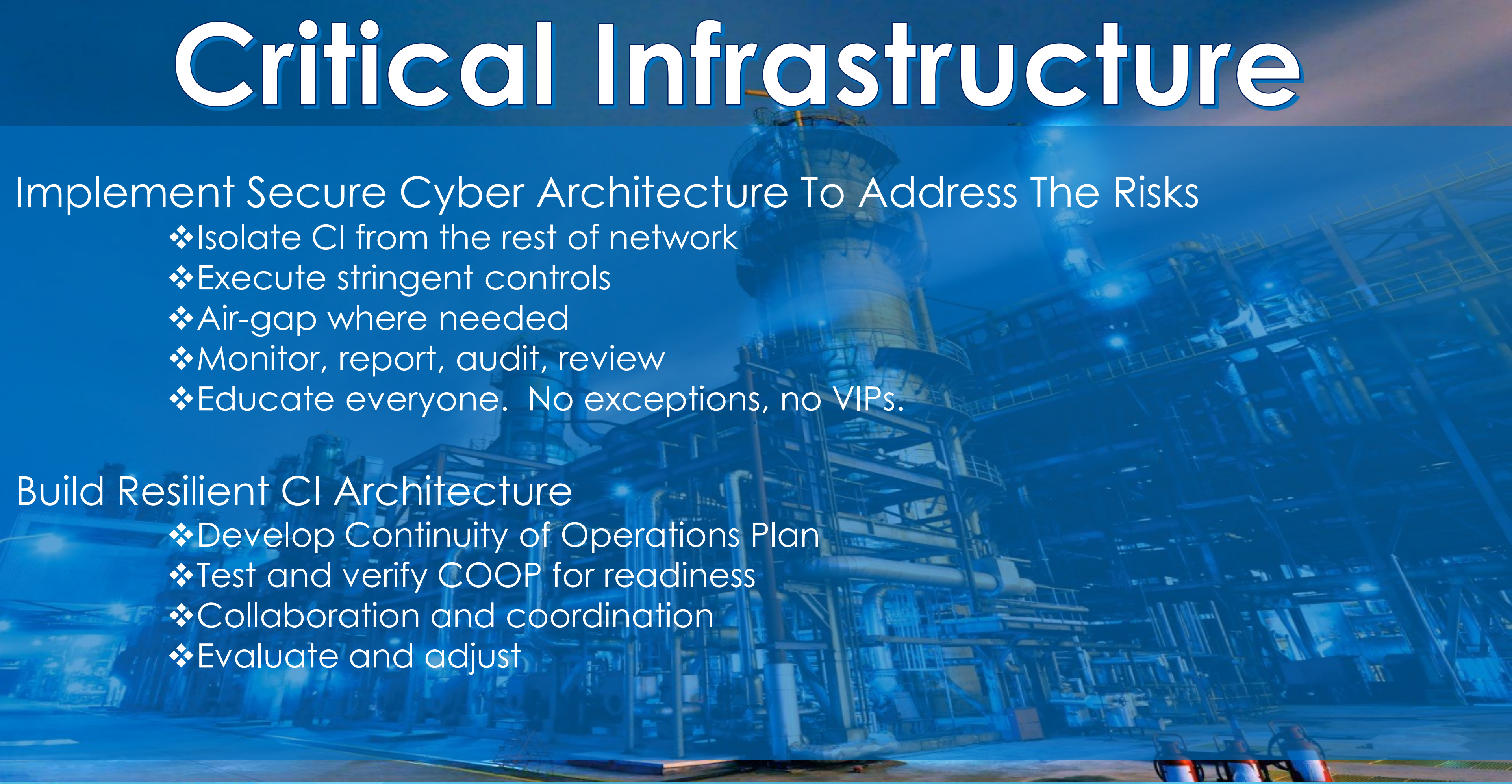
Other Security Solutions

IDS/IPS, DLP
Identity Management, Two-factor authentication
Forensic tools

User Security Awareness

Educating Users & Leadership
Security Awareness Day
Program & Sessions
Annual Security testing

Critical Infrastructure

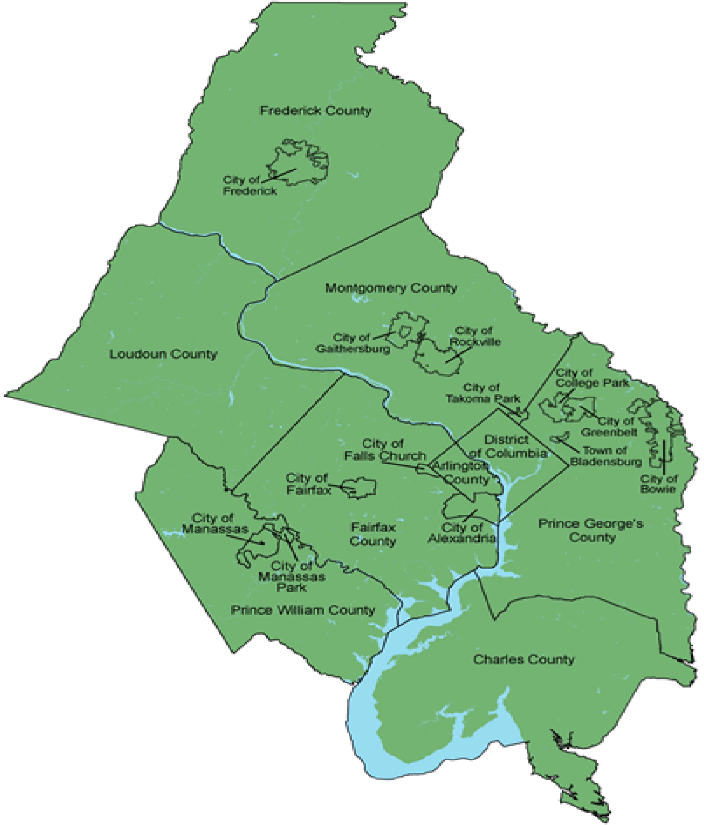


Implement Secure Cyber Architecture To Address The Risks

- ❖Isolate CI from the rest of network
- ❖Execute stringent controls
- ❖Air-gap where needed
- ❖Monitor, report, audit, review
- ❖Educate everyone. No exceptions, no VIPs.

Build Resilient CI Architecture

- ❖Develop Continuity of Operations Plan
- ❖Test and verify COOP for readiness
- ❖Collaboration and coordination
- ❖Evaluate and adjust



NCRNET

NCRnet is an interconnection of existing jurisdictional networks

Interoperable Data Communications

Who is part of NCRNET?

- All NCR/COG jurisdictions are part of NCRnet. In addition, NCRnet peers with networkMaryland, and interconnects with MWAA, MWATA, MWCOG, and VDOT

NCRNET Security

- Controlled & Secure Private Network

Proven Results

- Allowed Secure Access to Social Media
- Allowed Secure access to approved Cloud applications
- Successful Server Consolidation Virtualization efforts
- Increased Security Threat & Incident Detection
- Decrease in Security Incidents
- Secure ioT and Critical Infrastructure

Questions

Please wait for the **microphone** before asking your questions

State your **name & organization**

Please don't forget to…

Complete the Post Event Survey

Thank You

OSIsoft®