"To care for him who shall have borne the battle..."

UNITED STATES DEPARTMENT OF VETERANS AFFAIRS
Office of Information Security

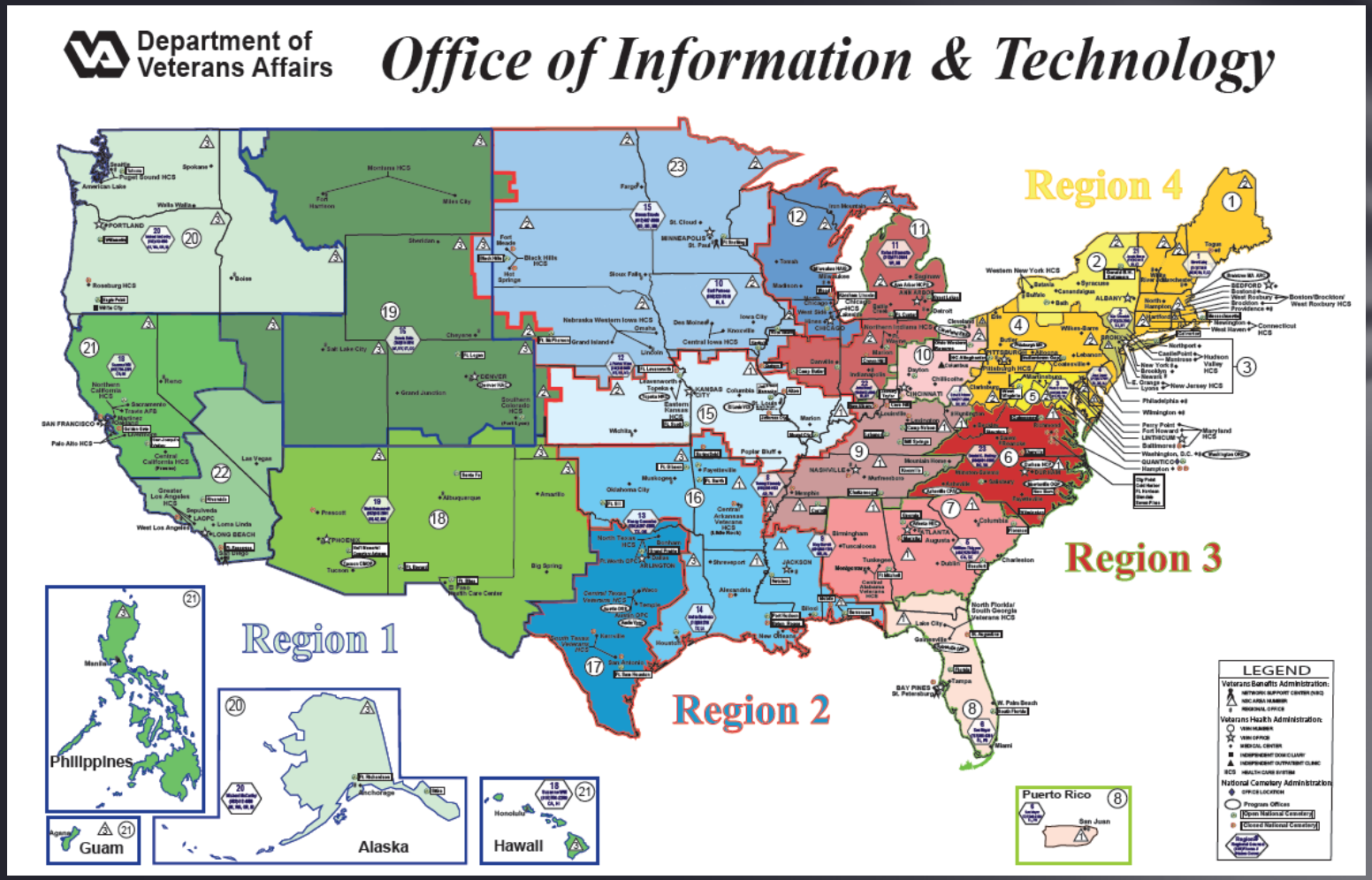
Enterprise Visibility

Continuously monitoring a network of over

400,000 users, and over 700,000 devices…

Department of Veterans Affairs

Office of Information & Technology



CRISP
Continuous Readiness in Information Security Program

152 Hospitals, 802 CBOCs, 293 Vet Centers,
131 Cemeteries, 56 Benefit Offices, 22M+ Vets

How we got here…

- Piloted Juniper/BigFix Remediation
- Ended up with Cisco/BigFix
- Mr. Roger Baker, VA CIO, October 6, 2010
  - Senate Committee on Veterans Affairs

    "Our network supports over 400,000 users, and over 700,000 devices… To vastly improve our information security posture, this spring we embarked on a project to provide visibility to every desktop on the network by the end of the fiscal year. I am pleased to report that we achieved that goal…we will achieve full visibility to every device on our network during fiscal year 2011."
- Visibility to Desktops (V2D) Initiative, 90 days, completed 9/30/2010

Genesis of Enterprise Visibility Dashboard

- Initial dashboard (Cognos) after V2D (BigFix) effort
  - Manual imports (.csv)
- IBM/Intelligent Decisions delivered ETL
  - Centralized reporting for 2 TEM Cores (~200K endpoints each)
  - Daily extracts, stores 60 days of TEM data
  - ETL (MS SQL SIS) - select properties and fixlets from TEM cores
- Next delivery - automated imports/reports
  - Executive level reports, 95% compliance threshold, 5 core apps
  - Drillable reports - Region, VISN, and Facility level

Enhancements to Delivered Capabilities

- VA Enterprise Visibility Team – BigFix/ETL/Cognos
  - New reports, capabilities, and enhancements
  - BAH SMEs - 5 Platform, 2 Development, 1 DBA/Tech Lead
- Visibility to the Server (V2S) – 90 days, 9/30/2011
- V2D and V2S Vulnerability Management
  - Top vulnerabilities
  - Key control and vulnerability trending (Cognos Metrics Studio)
  - Mobile Reports - Cognos Mobile license and Active Reports

Enhancements to Delivered Capabilities

- Active Directory (AD) Authentication
  - Multi AD domain access to restricted areas (machine-level)
- Common Vulnerabilities and Exposures (CVE) Reporting
- Software Installation and Version Reporting
  - Based off of custom relevance written by EV Team and pulled via ETL
  - Standardized relevance/reporting
  - 4 day new report turn around time request to production

Additional Integration Points

- Common Vulnerability Scoring System Integration (CVSSv2)
  - Web Services module risk scoring interface
  - Integrated V2D and V2S data at VA Enterprise, Region, VISN, or Facility Level.
- Inline/Context Sensitive - custom JavaScript
- Visibility to the Network (V2N) – SolarWinds (NPM/NCM)
- Incident Response Reporting
  - Privacy/Security Event Tracking System (BMC Remedy)
  - Laptop encryption and loss trending

BigFix Environment

- 400,000 Managed Nodes
  - 380,000 Desktops (Workstations and Laptops)
  - 20,000 Servers (Windows, Linux, Sun, HP, AIX, Mac)
- 524 Relays, 14 Top Level Relays, 16 DMZ Relays, 2 Core Servers, 2 Web Reports Servers, 2 TEMA Servers
- 75 Console Users, 1200 Web Reports Users, 65 TEMA Users

Future Direction and Development

- Dashboard 2.0 – New look/Feel, ArcGIS integration
- GRC Integration/Information Security Continuous Monitoring (ISCM)
- Continued Expansion of Customized Reporting
- Additional Data Integration Points – Nessus, EMF-FDR
- Visibility to Everything (V2E)
- Line of Business?

Lessons Learned

- More data in TEM than pulled via ETL, valuable w/understanding of TEM schema
- Client Posture Assurance – NAC, GPO, Client Deploy Tool, Manual, O&M Plan
- Limit console accounts, key to CM, hard to break "owner" mindset
- Balancing of nodes reporting to top level relays, limit direct reporting to cores
- Automated client scripts/policies in place prior to deployment to sort the endpoint population and limit WAN bandwidth usage
- Ongoing performance maintenance is needed, keeping ahead of demand
- O&M plan should be in place to ensure coverage of all endpoints is sustained.
- Need checks and balances – use additional tool(s) to verify
- Get a good count of systems (scan) for license buy, negotiate hard, get SUA if you can!!!
- Reporting needs work
- More to be shared (after session)