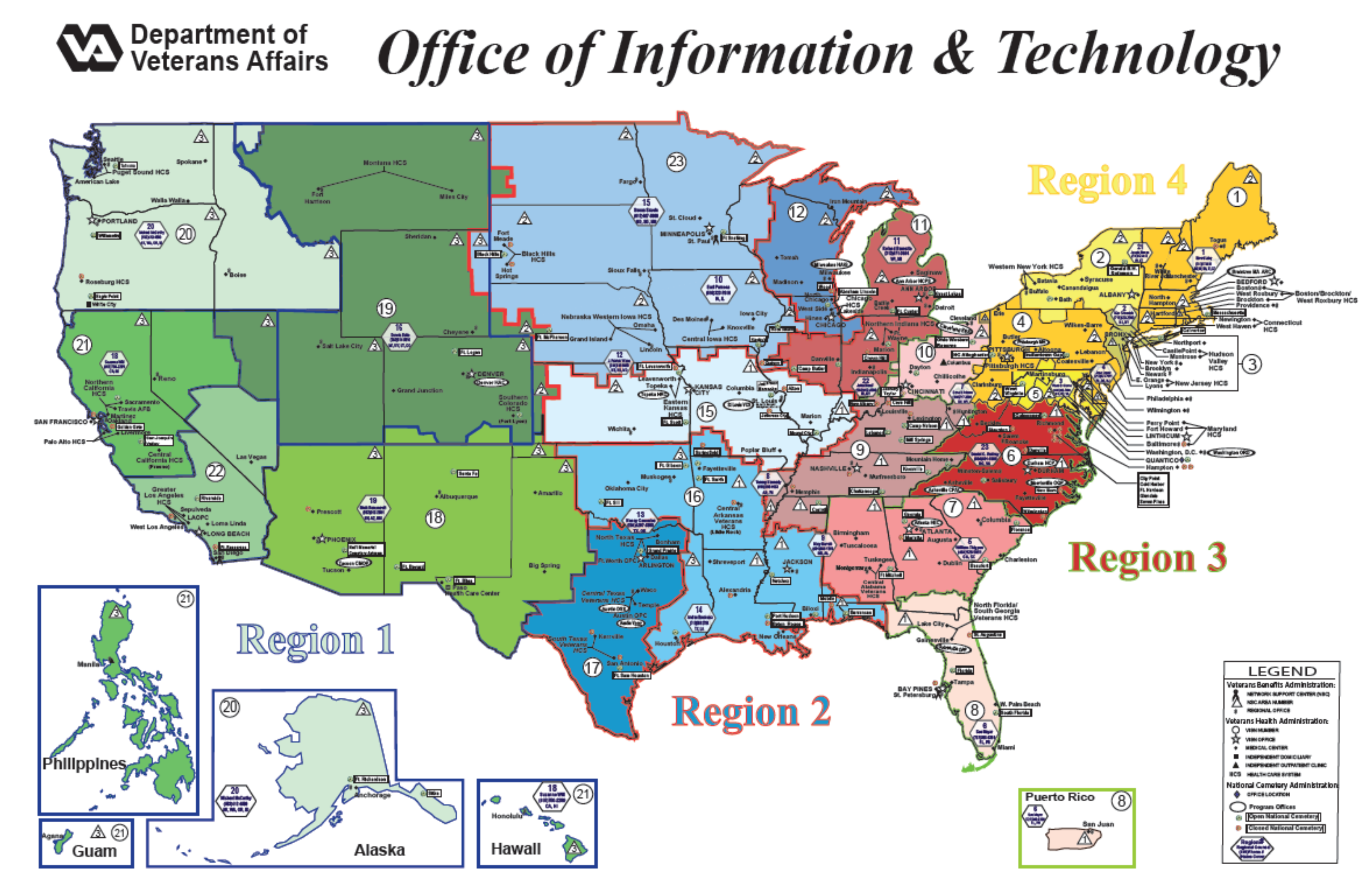
"To care for him who shall have borne the battle..."

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…

CRISP
Continuous Readiness in Information Security Program


Department of Veterans Affairs
Office of Information & Technology
Region 1
Region 2
Region 3
Region 4
Philippines
Guam
Alaska
Hawaii
Puerto Rico
LEGEND
Veterans Benefits Administration
Veterans Health Administration
National Cemetery Administration

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

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 Security Analytics Servers
- 75 Console Users, 1200 Web Reports Users, 65 Security Analytics Users

Lessons Learned

- More data in TEM than pulled via ETL, understand BigFix 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
- Endpoint O&M plan
- Need checks and balances? – use additional tool(s) to verify, build trust
- Get a good count of systems (scan) for license buy, negotiate hard, get SUA! It will pay for the tool
- Reporting needs work

GRC Tool Integration

- Awarded 9/27/12 – Agiliance Risk Vision
- Highlights
  - Initial Operating Capability – 60 days
    - Pre-built connectors for *most* our products
      - BigFix, SolarWinds, Tenable, Remedy, etc.
    - Fully user configurable – little to no programming needed, wizards
    - JasperSoft Reporting/Analytics/Dashboard/Cognos Integration
    - Open-standards platform, published schema
    - Hadoop layer for multiple network data source indexing and filtering for discovery of differential patterns and multidimensional relationships, as well as a Network Risk Analytics data-mart to produce the risk Visualization dashboards and reports
    - Hive, ZooKeeper and other open source