DOC 013

National Cyber Initiative

January 2009

Overall Classification: ~~SECRET//NOFORN~~
This Slide: ~~UNCLASSIFIED/FOR OFFICIAL USE ONLY~~

National Imperative

- Pre-2007 the threat was recognized, but no substantive cross-governmental effort existed on a sufficient scale to address that threat
  - In the face of ongoing intrusions coordinated decisive action was needed
  - No longer sufficient to discover intrusions, clean up the damage, and take legal or political steps to deter further intrusions
  - We must take proactive measures to detect and prevent intrusions before they can cause significant damage

- *We were at a “tipping point”*
  - Globalization has exposed our information technology/networks to foreign access and influence at a time when malicious cyber activity grows more extensive and sophisticated
  - This technology was not designed with security in mind, we need to lead the world to a new resilient information architecture that would make our infrastructure easy to use, safe, hard to break, and quick to recover

National Approach

- Beginning May 2007, the National Cyber Study Group (NCSG) was formed consisting of over 20 Departments and Agencies and formulated a new strategy
  - Strengthen our defenses by providing insight from our own offensive capabilities
  - Marshal our intelligence collection to prevent intrusions before they happen
  - Draw upon the full capabilities of law enforcement, intelligence, military, diplomacy, and cybersecurity

- January 8, 2008, President Bush issued National Security Presidential Directive 54/Homeland Security Presidential Directive 23, which formalized the "Comprehensive National Cybersecurity Initiative (CNCI)"

ODNI / Cyber

- Joint Interagency Cyber Task Force (JIACTF)
  - Formed by ODNI to coordinate across departments/agencies
  - Working Groups & Detailees from DHS, State, IC, DoD, DoJ, DOE, and others
  - Information Sharing
    - Quarterly Reporting/ Weekly SITREPs
  - Continuous Engagement
    - Private Sector is critical element leading to true success
    - Congress
    - Executive Branch (NSC-HSC)
  - Focus is on developing a preventative systemic capability

CNCI

- Strengthen Defense of our networks
  - Reduce vulnerabilities and prevent intrusions
  - 12 Initiatives & 7 Enablers
  - Leap-ahead technologies

(b)(1)(b)(3) NSA

[redacted]

[redacted]

(b)(1)(b)(3) CIA

(b)(1)(b)(3) NSA & CIA

[redacted]

Challenges

- Maintaining Momentum
- Building:
  - Enduring strategic framework
  - Public-private and international alliances
  - Trust into our information infrastructure
- Strengthening mechanisms to:
  - Monitor execution and mitigate execution risk
  - Share information, resources, and capabilities between offense, defense, and investigative activities
  - Explore technology development
  - Facilitate common practices between Federal organizations
  - Broader development of operational knowledge and skills
  - Maximize benefit of existing centers of excellence
  - Quantify the economic consequences of the problem
- Engage the American public to:
  - Increase awareness of their role in cyberspace safety & security

- Back-up

Non-responsive

[redacted]

[redacted]

Non-responsive

[redacted]

[redacted]

[redacted]

~~SECRET//NOFORN//20320108~~