WAYNE M. MURPHY
DIRECTOR OF OPERATIONS

PRESIDENT ELECT IC TRANSITION TEAM
CYBER BRIEF

Approved for Release by NSA on 02-22-2018

THE OVERALL CLASSIFICATION OF THIS BRIEF IS
~~TOP SECRET//SI//ORCON/NOFORN~~

PL 86-36/50 USC 3605

(U) NSA CYBER OPERATIONS FUNCTIONS

(U//~~FOUO~~) NSA conducts 24/7 network defense activities to discover, characterize and counter threats to U.S. national security systems

- (U) Foreign Intelligence (50 USC § 3038(b)(1), EO 12333, FISA)
  - Provides unparalleled insight into adversary's plans, intentions, and operations
- (U) Information Assurance (EO 12333, NSD-42, EO 13587)
  - Advances security architectures, develops and operates unmatched cyber defense capabilities and services, examines National Security Systems and evaluates their vulnerability to foreign exploitation

(U) NSA DEFENSE OPERATIONS

PL 86-36/50 USC 3605

(U//~~FOUO~~) NSA provides Computer Network Defense (CND) services. NSA currently has services deployed on National Security Systems, the Department of Defense Information Network (DoDIN) [redacted]

[redacted]

- (U) Strategic Vulnerability Discovery
  - Comprehensive assessment of network vulnerabilities
  - NSA leverages threat intelligence to strategically assess networks
- ~~(S//REL~~) Hunting and Finding
  - Persistent and on demand search for adversarial tactics, techniques and procedures and tradecraft
  - NSA postures itself in critical networks to identify advanced threats embedded in USG networks
- (U//~~FOUO~~) Authorized Hacking
  - Emulation of advanced persistent threat (APT) Tactics, Techniques, and Procedures (TTPs)
- (U//~~FOUO~~) Incident Responses
  - Rapid deployment of cyber investigative and forensic capabilities to compromised sites

[redacted]

(U)NSA FINDINGS IN THE NATIONAL SECURITY DOMAIN

PL 86-36/50 USC 3605

(U//~~FOUO~~) **NSA conducted [redacted] vulnerability assessments/authorized hacking operations in 2016** using a combination of commercial and government tools. During these operations NSA continues to find routinely that basic cyber security “best practices” have not been implemented, or have been poorly implemented, in networks critical to U.S. National Security.

(U) Common vulnerabilities present in customer networks include:

- Use of default usernames/passwords (e.g., “admin”)
- Unpatched and end-of-life applications
- Clear text network protocols that disclose usernames/passwords
- Vulnerable unauthorized software
- Use of USB devices leading to cross domain violations
- Password re-use across accounts/systems

EO 1.4.(g)
PL 86-36/50 USC 3605

U.S. FEDERAL CSO TEAM

Roles and Responsibilities

US GOVERNMENT DEPARTMENTS AND AGENCIES

DOJ/FBI

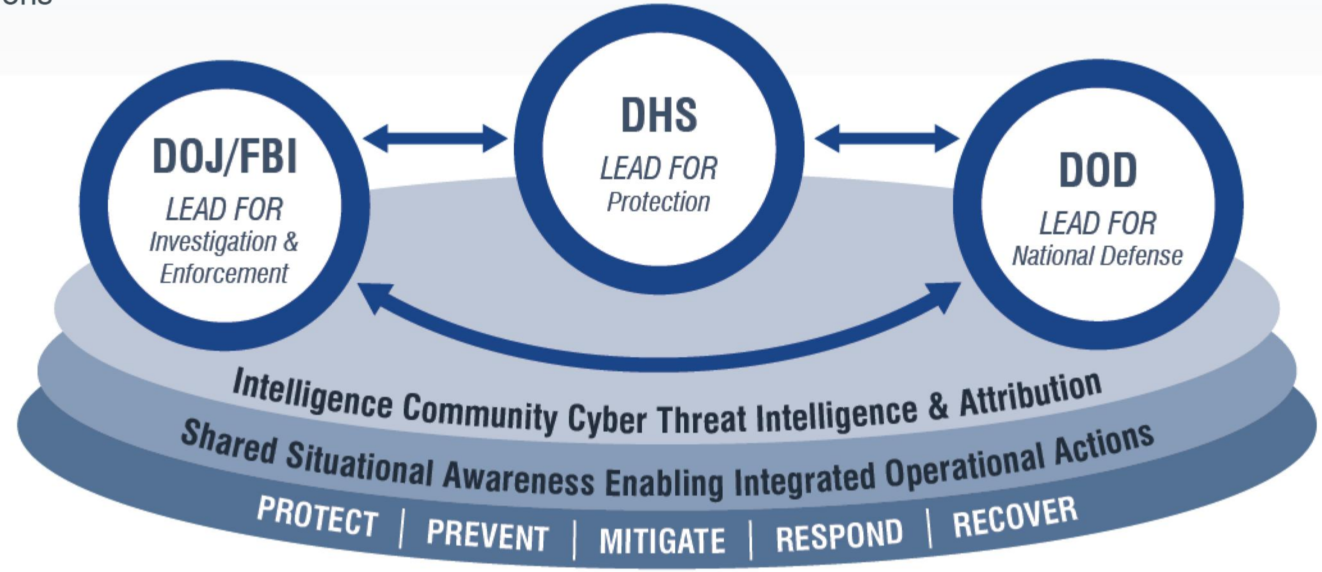
- Investigate, attribute, disrupt and prosecute cyber crimes
- Lead domestic national security operations
- Conduct domestic collection, analysis, and dissemination of cyber threat intelligence
- Support the national protection, prevention, mitigation of, and recovery from cyber incidents
- Coordinate cyber threat investigations

DHS

- Coordinate the national protection, prevention, mitigation of, and recovery from cyber incidents
- Disseminate domestic cyber threat and vulnerability analysis
- Protect critical infrastructure
- Secure federal civilian systems
- Investigate cyber crimes under DHS's jurisdiction

DoD

- Defend the nation from attack
- Gather foreign cyber threat intelligence and determine attribution
- Secure national security and military systems
- Support the national protection, prevention, mitigation of, and recovery from cyber incidents
- Investigate cyber crimes under military jurisdiction



DOJ/FBI
LEAD FOR
Investigation & Enforcement

DHS
LEAD FOR
Protection

DOD
LEAD FOR
National Defense

Intelligence Community Cyber Threat Intelligence & Attribution

Shared Situational Awareness Enabling Integrated Operational Actions

PROTECT | PREVENT | MITIGATE | RESPOND | RECOVER

GLOBAL CYBERSPACE

Coordinate with Public, Private, and International Partners

*Note: Nothing in this chart alters existing DOJ, DHS, and DoD roles, responsibilities, or authorities

Doc ID: 6611716

(U) CHALLENGES

PL 86-36/50 USC 3605

- (U) Fragmented cybersecurity authorities/responsibilities across the USG

[redacted]

- (U//~~FOUO~~) Getting classified, actionable data into non-National Security System domains
- (U) Salary/incentive limitations for employees with critical cybersecurity skills

(U) RECOMMENDATIONS

EO 1.4.(c)
PL 86-36/50 USC 3605

- (U//~~FOUO~~) Unified and coherent cyber defense framework for the USG
  - Potentially one USG agency as the cyber defense execution lead
  - Policies/authorities/directives architecture that effectively prosecutes cybersecurity mission while also ensuring protection of U.S. Persons' privacy

[redacted]

  - Resources would need to be adjusted accordingly
- (U//~~FOUO~~) Scale actionable cyber threat intelligence sharing b/w all USG elements [redacted]

PL 86-36/50 USC 3605

- (U) Increased investment in technically skilled people and advanced technologies

GREG SMITHBERGER
DIRECTOR OF CAPABILITIES
and
CHIEF INFORMATION OFFICER
NATIONAL SECURITY AGENCY

PRESIDENT ELECT IC TRANSITION TEAM
DEFENSIVE MEASURES BRIEF

THE OVERALL CLASSIFICATION OF THIS BRIEF IS
~~TOP SECRET//SI//NOFORN~~

EO 1.4.(c)
PL 86-36/50 USC 3605

DEFENSIVE MEASURES

Responding to Unauthorized Disclosure Events

EO 1.4.(c)
PL 86-36/50 USC 3605

EO 13587 (October 2011)

[redacted]

Secure the Net (July 2013)

[redacted]

Secure the Enterprise (September 2015)

[redacted]

Enhanced Insider Threat Defensive Measures (October 2016)

[redacted]

ENHANCED INSIDER THREAT DEFENSIVE MEASURES

EO 1.4.(c)
PL 86-36/50 USC 3605

[redacted]

- ~~(C//REL)~~ Perform Data Segregation and Sanitization [redacted] [redacted]
- ~~(C//REL)~~ [redacted] employing enhanced physical security barrier/procedures, including Two-Person Procedures
- ~~(C//REL)~~ Enhance Personnel Reliability and Suitability based on work roles to maintain vigilance on residual risks
- (U//~~FOUO~~) Engage Workforce to reinforce balance between Mission, IT and Security

SECURITY DRIVEN RESPONSE

PL 86-36/50 USC 3605

- **Education and Training**
  - (U) Enhance training to promote a ‘Culture of Security’ and responsibility of all to report anomalous affiliate behavior
- **Human Resources**
  - (U//~~FOUO~~) [redacted] research and implement new [redacted] tools/instruments; [redacted]
  - (U//~~FOUO~~) Adjust civilian hiring [redacted]

EO 1.4.(c)
PL 86-36/50 USC 3605

- **Installations and Logistics**
  - [redacted]
  - ~~(C//REL)~~ Enhance property accountability [redacted]
- **Security & Counterintelligence (S&CI)**
  - (U//~~FOUO~~) IC Security policy adjustments and personnel security reforms (investigations, adjudications, polygraph)
  - (U//~~FOUO~~) Focused Industrial Security inspections [redacted]
  - [redacted]

QUESTIONS?

Doc ID: 6611716

~~CONFIDENTIAL//REL TO USA, FVEY~~

November 2016

Secure the Enterprise Initiatives

EO 1.4.(g)
PL 86-36/50 USC 3605

[redacted]

Maintain a Secure Enterprise

Objectives	Complete
[redacted]	[redacted]

Actively Defend the Enterprise

Objectives	Complete
[redacted]	[redacted]

Integrate Enterprise Expertise

Objectives	Complete
[redacted]	[redacted]
7.2 (U) Inform the Enterprise of "Secure the Enterprise" strategy and details (with reinforcement in subsequent communications).	Complete
7.3 (U) Develop and implement a comprehensive plan to drive culture change.	Ongoing
[redacted]	[redacted]

[redacted]

Goal: "NSA is the USG Standard for How Networks Should be Built, Operated, Secured, & Defended"

[redacted]

~~CONFIDENTIAL//REL TO USA, FVEY~~

(U) Legend: **Black Text** – complete **Blue Text** – ongoing

Doc ID: 6611716

Secure the Net Initiatives

August 2016

EO 1.4.(g)
PL 86-36/50 USC 3605

Tighten Control on Computer Systems - 12

Objectives	Complete
CURRENT/LEGACY ARCHITECTURE	
[redacted]	
[redacted]	
CURRENT/LEGACY & FUTURE ARCHITECTURE	
[redacted]	
FUTURE ARCHITECTURE	
[redacted]	
[redacted]	

Tighten Control on Data - 7

Objectives	Complete
CURRENT/LEGACY & FUTURE ARCHITECTURE	
[redacted]	
FUTURE ARCHITECTURE	
[redacted]	
[redacted]	

(U) Legend

Black Text – complete

Blue Text - ongoing

Increase Oversight of People - 21

Objectives	Complete
CURRENT/LEGACY ARCHITECTURE	
CURRENT/LEGACY & FUTURE ARCHITECTURE	
[redacted]	
[redacted]	
(U) Adjudicative Review	Complete
[redacted]	
FUTURE ARCHITECTURE	
[redacted]	