All FBI information contained
herein is unclassified
09/16/2021 by [redacted] NSICG

(b)(6)-1 per FBI
(b)(7)(C)-1 per FBI

Document ID: 0.7.148.5160

From: Hickey Adam NSD USA GOV
(b) (6)

To: Gauhar, Tashina (b) (6)
[redacted]

Cc:

Bcc:

Subject: FW: NSD Cyber Transition Binder --- ~~TOP SECRET//SI//NOFORN~~

Date: Tue Apr 11 2017 19:48:31 EDT

Attachments: Tab D - Significant Cyber Incidents and Responses 03-2017 FINAL.pdf
Tab E - Cyber Operations and Framework 03-2017.pdf
Tab F -- LP Cyber Portfolios 03-2017 FINAL.pdf

Classification: ~~TOP SECRET//SI//NOFORN~~

Classified By: Hickey Adam NSD USA GOV
Derived From: DOJ/NSI SCG 1 INT dated 20120701
Declassify On: 25X1, 20671231
==

==
Classification: ~~TOP SECRET//SI//NOFORN~~

~~TS\SCI Classified~~.

(b)(6)-1 per FBI
(b)(7)(C)-1 per FBI

All FBI information contained
herein is unclassified
09/16/2021 by [redacted] NSICG

Tab D: Significant Cyber Incidents and Responses

(U) The United States relies on the Internet for a wide range of services. The internet not only provides a backbone for many of our national defense activities, but it is also the foundation for much of the United States' critical infrastructure, connecting to the systems that support the energy sector, banking and financial services, communications, and transportation, among others. Despite the pivotal role it plays in everyday life, the internet was not built with security in mind. As interconnectivity spreads, so has the opportunity for state and non-state actors to exploit the internet's vulnerabilities. Over the past eight years, the U.S. government (USG) has used a variety of tools — including attribution, information sharing, technical operations, sanctions, and prosecution — to deter, combat, and respond to malicious cyber activities targeting the United States and its institutions.[1]

Excluded per agreement

[1] ~~(TS//NF)~~ [redacted]

(b)(3)-1 per FBI
(b)(7)(E)-1,-3 per FBI

Excluded per agreement

Excluded per agreement

Russia

(~~C//NF~~) **Incidents:**

Excluded per agreement

Excluded per agreement

(b)(7)(E)-1 per FBI

- (U) July – Nov. 2016 – [redacted] Emails from the Democratic National Committee (DNC) server were subsequently hacked and posted to WikiLeaks and other online outlets (such as DCLeaks) in the form of information releases and a searchable database. Hackers also secured access to the email account of John Podesta, Hillary Clinton's campaign chair, and WikiLeaks and other online outlets began releasing batches of Podesta's emails.

Excluded per agreement

~~(TS//NF)~~ **USG Responses:**

- (U) *Indicator release:* [redacted]

(b)(7)(E)-1 per FBI

- (U) *Attribution:* Oct. 2016 – Jan. 2017 – the United States formally accused the Russian government of stealing and disclosing emails from the Democratic National Committee in an effort to influence the U.S. election process. Specifically, on October 7, 2016 ODNI and DHS released a public statement indicating that the U.S. Intelligence Community (USIC) was "confident" that the Russian Government directed the compromises of e-mails from US persons and institutions, including e-mails from US political organizations, which were subsequently released on sites like DCLeaks.com and WikiLeaks. The statement indicated that the thefts and disclosures were intended to interfere with the U.S. election process and that only Russia's senior-most officials could have authorized these activities. On December 29, 2016, FBI and DHS publicly released a Joint Analysis Report on "GRIZZLY STEPPE – Russian Malicious Cyber Activity" (the "JAR"), which provided technical details regarding the tools and infrastructure used by the Russian civilian and military intelligence services to compromise and exploit networks and endpoints associated with the U.S. election, as well as a range of U.S. Government, political, and private sector entities. On January 6, 2017 ODNI publicly released a detailed intelligence community assessment entitled "Assessing Russian Activities and Intentions in Recent US Elections." The assessment, which was authored and coordinated among the CIA, the FBI and the NSA, concluded with "high confidence" that Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the U.S. presidential election.

- (U) *Sanctions:* Dec. 2016 – In response to Russian interference with the 2016 presidential elections, President Obama approved an amendment to E.O. 13964 to authorize sanctions on those who "tamper with, alter, or cause a misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions." Under this authority, the President sanctioned nine entities and individuals, including two Russian intelligence services (the GRU and the FSB), four individual officers of the GRU, and three companies that provided material support to the GRU's cyber operations. The Obama administration also expelled 35 Russians suspected of being intelligence operatives "persona non grata." In addition, the Secretary of the Treasury designated two Russian individuals (one of whom was, as discussed below, later charged in relation to the Yahoo intrusions) for using cyber-enabled means to cause misappropriation of funds and personal identifying information; the State Department shut down two Russian compounds used for intelligence-related purposes; and DHS and FBI released declassified technical information on Russian civilian and military intelligence service cyber activity to help network defenders in the U.S. and abroad to identify, detect, an disrupt Russia's global campaign of malicious cyber activities.

- (U) Jan. 6, 2017 – DHS designated election infrastructure as a subsector of the existing Government Facilities critical infrastructure sector. This helps ensure that election infrastructure will receive prioritized cybersecurity assistance from DHS should state or local officials request it. "Election infrastructure" includes storage facilities, polling places, centralized vote tabulations locations used to support the election process, information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and report and display results on behalf of state and local governments.

Excluded per agreement

Excluded per agreement

Excluded per agreement

Excluded per agreement