

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26

**UNITED STATES DISTRICT COURT  
DISTRICT OF ARIZONA**

Kari Lake; Mark Finchem,  
Plaintiffs,

v.

Kathleen Hobbs, as Arizona Secretary of  
State; Bill Gates; Clint Hickman; Jack Sellers;  
Thomas Galvin; and Steve Gallardo, in their  
capacity as members of the Maricopa County  
Board of Supervisors; Rex Scott; Matt Heinz;  
Sharon Bronson; Steve Christy; Adelita  
Grijalva, in their capacity as members of the  
Pima County Board of Supervisors,  
Defendants.

No. 2:22-cv-00677-JJT

**DECLARATION OF JOHN R. MILLS**

1 I, John R. Mills, declare under penalty of perjury that the following is true and correct:

2 1. I have personal knowledge of the matters set forth below and could and would testify  
3 competently to them if called upon to do so.  
4

5 **Introduction**

6 2. I am Colonel, USAR, (Retired), John R. Mills and also Former Director of Cybersecurity  
7 Policy, Strategy, and International Affairs, Office of the Secretary of Defense, Senior Civilian  
8 (Retired). My dual career as an Active and Reserve member of the U.S. Army as well as a senior  
9 civilian in the Department of Defense has given me a unique opportunity for almost 40 years to  
10 participate directly in, provide oversight of, or be aware of a vast array of the planning and use of a  
11 wide range of U.S. cybersecurity-related instruments of national power. I have held Top Secret,  
12 Sensitive Compartmented Information (SCI) security clearances since approximately 1988. I have also  
13 been an adjunct Professor and have taught graduate level cybersecurity law and policy since 2013 at  
14 the University of Maryland, Global Campus. My last uniform position in the Department of Defense  
15 was in Homeland Defense and I often served as a liaison with Department of Homeland Security to  
16 coordinate the national response to complex emergencies and threats to the Homeland (real events and  
17 exercises).  
18

19 3. I have been asked in this case to testify on the development, capabilities, and uses of “remote  
20 access operations” for unlawful entry and purposes into computer networks. The information  
21 presented is unclassified and based upon my personal experiences, publicly available reporting,  
22 studies, events, incidents, best practices, and de-classified U.S. Government information.  
23

24 4. Remote access operations refer generally to the activities used to access computer networks,  
25 data centers, and other equipment, conducted in a manner to avoid detection and avoid leaving behind  
26

forensic evidence of the access. Remote access operations are often enabled by planted malware, enabling software, and/or algorithms in the targeted computer system.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26

5. Remote access operations are different from remote maintenance monitoring which is intended by network designers for transparent and auditable access to network enabled devices for maintenance and updates. However, remote maintenance monitoring can be subverted or co-opted for reasons not in accordance with remote maintenance monitoring tenets, design intent, network owners/operators, or lawful access/purpose.

6. From the 1980s to the present, the capabilities, scope, and scale of remote access operations to collect or alter data have greatly expanded. The offense in remote access operations (the person or government seeking unauthorized access to a computer network) normally has a decided advantage against defenders (the person or government seeking to prevent unauthorized access).

7. The U.S. Government conducts remote access operations through the entities described in Executive Order 12333<sup>1</sup>, as described in the articulation of the U.S. Intelligence Community<sup>2</sup> roles, missions, and organization, and as directed by a sitting President. The U.S. Intelligence Community is enabled by and often operates in close coordination with the Department of Defense and Federal Law Enforcement for these operations.

8. Other countries, organizations, and individuals have also developed remote access operation capabilities with varying degrees of sophistication. Such capabilities have been expanding at an accelerating rate in the past 20 years. These operations have become ubiquitous through nation state and private actors.

---

<sup>1</sup> Presidential Executive Order 12333 United States Intelligence Activities (As amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008)); <https://irp.fas.org/offdocs/eo/eo-12333-2008.pdf>

<sup>2</sup> EPIC.org, “Background on Executive Order 12333”; <https://archive.epic.org/privacy/surveillance/12333/>

1 9. Electronic election infrastructure is one example of critical infrastructure<sup>3</sup> which can be  
2 subjected to remote access operations. Foreign remote access operation capabilities threaten critical  
3 infrastructure in the United States, such as election systems.

4 10. A successful remote access operation conducted against U.S. election infrastructure could  
5 change vote totals reported by the election equipment, thereby nullifying the election as an expression  
6 of the collective will of the voters.

7 11. The employment of machine-based algorithms to access electronic voting systems in the United  
8 States to impose a pre-determined election outcome through remote access operations is well within  
9 the capabilities of many nation-state actors such as China, Russia, Iran, and Venezuela, as well as even  
10 non-nation state actors.

11 12. I have reviewed the Mesa County Forensic Reports (Reports 1, 2, and 3) concerning the  
12 examination of images of the hard drives of the Dominion Voting System (DVS) Democracy Suite (D-  
13 Suite) version 5.11-CO Election Management System (EMS) server of Mesa County, Colorado. The  
14 DVS D-Suite EMS server in that configuration was used for all Mesa County elections held in 2020  
15 and through May 2021, including the November 2020 General Election, and the April 2021 Grand  
16 Junction Municipal Election.

17 13. My conclusions from reviewing these Reports are detailed below, and in my opinion, the  
18 evidence found on the Mesa County server is consistent with either remote access operations and/or  
19 the employment of sophisticated algorithms.

20  
21 **Summary**  
22  
23  
24

---

25 <sup>3</sup> CISA Website, Election Infrastructure as Critical Infrastructure, <https://www.cisa.gov/election-security>  
26

14. The U.S. Government has pioneered and advanced the art and techniques of remote access operations targeting critical infrastructure.

15. Based on my personal experience the United States Government has the capability to project significant effects<sup>4</sup> toward critical infrastructure worldwide—including election systems. This same capability (to project effects) now exists in other countries, such as China, Russian, Iran, North Korea, and Venezuela, and these foreign powers now use these same, similar, and improved remote access operation methodologies to advance their own national agendas.

16. These operations have created a growing talent base of personnel, software, and network enabled capabilities that are becoming ubiquitous in the hands of companies and personnel outside of the U.S. Government.

17. I have served as a sworn election official and understand the U.S. election process at the county level. With that experience and my professional experience, I have very low confidence in the security of American election critical infrastructure. In my professional opinion, assertions by the U.S. Intelligence Community, Homeland Security, and other law enforcement officials that they have the situational awareness and capability to defend the election environment against remote access operations with a high level of confidence are unsupported and, in some cases, may be false. Several publicly known breaches of critical infrastructure are presented later in this document. One of the most damaging and egregious was the breach of the Office of Personal Management which created catastrophic results. The full resources and full spectrum of the U.S. Government were available to detect, prevent, stop, mitigate, or otherwise address the attack on this critical infrastructure, yet the attackers circumvented all measures designed to stop them.

---

<sup>4</sup> “Effects” is an operator’s and planner’s term of art which implies the ability to degrade, exfiltrate, manipulate, change, or destroy.

18. My professional opinion is that the statement “The November 3rd election was the most secure in American history” asserted on November 12, 2020 on the Cybersecurity and Infrastructure Security Agency (“CISA”) website, had little, if any, basis in fact.<sup>5</sup>

19. In my professional opinion, based upon substantial experience on national cyber capabilities, cybersecurity, planning, policy, strategy, and review, and establishment of actionable recommendations for mitigation, policy, procedure, process, and remediation of multiple, large scale breaches and attacks on major critical network systems, and with my knowledge of the election process, the statements made by CISA referred to above, to be properly, independently, and holistically assessed must include a factual establishment and public release of the actual National Intelligence Collection priorities at the time of the November 2020 election, and the precise and specific signatures and indicators the national intelligence collection system (and law enforcement), and their capabilities were supposedly tracking, monitoring for, sensoring for, and otherwise tuned to monitor, collect, and defend the 2020 election.<sup>6</sup> The broad assertions and statements by Mr. Krebs and others also presume an ability to detect these remote access operations in an extremely timely manner with extremely high confidence—which is simply not realistic at this point in time and have a poor track record.

20. Regarding the Mesa County Forensic Reports, the findings are consistent with previous, publicly known, computer network intrusions, breaches, exfiltrations, and compromises of data integrity conducted via remote access operations by sophisticated actors, likely nation state level, with intimate, insider knowledge of the machines, networks, operating systems, and complete architecture of the information technology environment including off premise, “cloud” based storage and

---

<sup>5</sup> CISA, Joint Statement, November 12, 2020, <https://www.cisa.gov/news/2020/11/12/joint-statement-elections-infrastructure-government-coordinating-council-election>

<sup>6</sup> The code name of the operation(s), their planning documents, establishment of inter-agency roles and missions, and all coordinating instructions to include the detailed guidance on factual Intelligence Collection priorities, including signatures and indicators, must be made public.

processing. There are three key themes that the findings can be grouped into for proper understanding and context by the reasonably informed layperson.

- 1 a. Complex and large-scale changes to data conducted at an operating system level that are  
2 not detectable to a top-level operator of the system who does not have deep, technical  
3 knowledge of the operating system. An analogy is expecting the driver of a vehicle to be  
4 able to conduct complex diagnostics and complete repair of the entirety of their car,  
5 including modern advanced, embedded information technology.
- 6  
7 b. Computer data base changes of significant complexity, scope, and scale that indicate  
8 sophisticated automated algorithms, remotely conducted via network access (which may  
9 include wireless elements, or unique methods of entry). More simply stated, the person(s)  
10 conducting these activities did not need to physically touch the machines or off-site servers  
11 nor manually, hands on keyboard, manipulate lines of code or data, instead these were  
12 automated operations, done remotely, with algorithms to adjust data, from operating sites  
13 potentially across the world.
- 14  
15 c. Complicated operations described in these reports, even with advanced algorithms, are still  
16 resource intensive from a planning and execution perspective and are greatly enabled and  
17 simplified by an insider who already knows, to a line of code level, the operating system,  
18 network architecture, security measures, and all related matters. In unembellished terms, a  
19 trusted insider who can unlock the right doors and know which switches to flip, is one of  
20 the most desired assets sought after by the mission planner. In the cybersecurity world, this  
21 is what is known as the “Witting Insider.”  
22  
23  
24  
25  
26

### Relevant Experience and Qualifications

21. I have defended our Country since 1983. My service for our Nation ranges from the tactical level in combat to the strategic at the Office of the Secretary of Defense (DOD). I am a school trained and qualified Military Intelligence Officer, Psychological Operations Officer (PSYOP – a Special Operations Community Branch), Civil Affairs Officer (also a Special Operations Community Branch), and Public Affairs Officer. My role has essentially been as a national security strategic planner since approximately 2001. My service at the senior levels of the U.S. Government has included complex inter-agency proceedings and deliberations on cyber and cybersecurity and other government operations across the spectrum of instruments of national power; international partner negotiation of sensitive information sharing agreements (including the Five Eyes (FVEYS<sup>7</sup>)); and representing the Department of Defense at the National Security Council from mid 2008 to mid 2009 as NS/HSPD-54/23.<sup>8</sup>

22. In my uniformed service, civilian service, and post-U.S. Government service I have worked, planned, implemented, observed, and made recommendations in American elections and foreign elections. I have served as a sworn election official in my home county, Prince William County Virginia, multiple times, including the November 2020 election, where 74% of the votes were cast by absentee ballot in one of several forms. This meant that 74% of the ballots were handled at what is known as the Central Absentee Precinct (CAP), where thumb drives were used and re-used with few

---

<sup>7</sup> “The Five Eyes was formally founded in the aftermath of the Second World War, through the multilateral agreement for co-operation in signals intelligence (SIGINT), known as the UKUSA Agreement, on 5 March 1946.” Since this original agreement, Canada, Australia, New Zealand have been added as well as other countries for unique functional topics. <https://ukdefencejournal.org.uk/the-five-eyes-the-intelligence-alliance-of-the-anglosphere/>

<sup>8</sup> Department of Homeland Security, Fact Sheet: Preventing and Defending Against Cyber Attacks, October 18, 2011; <https://www.dhs.gov/news/2011/10/18/preventing-and-defending-against-cyber-attacks>



chain of custody procedures. The use of a thumb drive is a key enabler in cyber intrusions based upon the Agent BTZ<sup>9</sup> and possibly Stuxnet<sup>10</sup>. I have also had the opportunity to brief Commonwealth level officials in 2022 on a number of points of concern on the security of voting in Virginia, including machines, cloud enabled storage and processing of voting data, voting rolls, and other matters.

### **Taiwan Election in January 2020**

23. An exemplar of the conduct of a fair, transparent, and trusted elections was the January 11, 2020, election in Taiwan. Taiwan is subject to continuous acts of aggression and coercion by the Communist government of China, and its elections are a point of potential vulnerability to Chinese Communist interference.

24. I was a senior Cyber Liaison from the Department of Defense to the Taiwan Ministry of National Defense's Computer Emergency Response Team from 2014 to 2018. Often my meetings included representatives of the Taiwan National Security Council, Taiwan's analogue to the U.S. National Security Council. In this role, I learned much about the issues Taiwan faces from China.

25. After I retired from the military, I had the opportunity to provide advice for the January 2020 elections in Taiwan. One of my recommendation was to make the process as simple and transparent as possible by relying on paper ballots, hand counting, and minimization of any election machines. I advised that ballots be tabulated (when not hand counted) as transparently as possible. I advised that tabulation machines should have no other feature other than to tabulate the ballot. The machines should have no features other than simple tabulation, and no connectivity sub-components such as Bluetooth, modems, or anything else. Such a configuration limits remote access operations to unique

---

<sup>9</sup> Council on Foreign Relations, Cyber-Operations, "Agent.btz", November 2008  
<https://www.cfr.org/cyber-operations/agentbtz>

<sup>10</sup> CNET, Stuxnet delivered to Iranian nuclear plant on thumb drive", April 12, 2012,  
<https://www.cnet.com/news/stuxnet-delivered-to-iranian-nuclear-plant-on-thumb-drive/>

access methods such as 110- or 220-volt power cords (i.e., wall power that the machine is plugged into)<sup>11</sup>.

1  
2 26. The Taiwanese executed their election in 2020 flawlessly. A new law was passed,<sup>12</sup> and arrests  
3 were made of foreign influence operatives who were accepting foreign payments for influence of  
4 elections. The election was conducted in a model of transparent processes using manual processes to  
5 the greatest degree possible, enabled by the simplest of election machines and technology. The  
6 counting of ballots was done live, on television broadcasts, with multiple observers from both parties,  
7 showing the ballot as marked, before the ballot was passed through, and Jumbo-Tron Screens showing  
8 how the counts changed with each ballot after being passed through the tabulator.

### 9 10 **The History of Remote Access Operations**

11 27. Since the Second World War and the 1947 and 1949 National Security Acts,<sup>13</sup> the U.S.  
12 Intelligence Community and the U.S. Government have sought, for purposes of national defense, to  
13 obtain information from and send information into regions controlled by hostile governments. Remote  
14 access operations flow from this practice.

15  
16 28. In the early days of computer networks, connectivity often relied upon “dial up” connections  
17 through common copper phone that linked the computers. There were no firewalls, gateways, or  
18 cybersecurity, and really no thought to security at the time<sup>14</sup>. The thought of a non-compliant or  
19 hostile participant was not really considered. Why would anyone be malign?.

20  
21  
22 <sup>11</sup> The Hacker News, “Hacker can steal data from air-gapped computers through Power Lines, April  
23 12, 2018, <https://thehackernews.com/2018/04/hacking-airgap-computers.html>

24 <sup>12</sup> ABC News, “Taiwan passes law targeting Chinese Political Interference, December 31, 2019,  
25 <https://abcnews.go.com/International/wireStory/taiwan-passes-law-targeting-chinese-political-interference-67996333>

26 <sup>13</sup> DNI, “National Security Act of 1947”, <https://www.dni.gov/index.php/ic-legal-reference-book/national-security-act-of-1947>

29. Eventually, information technology engineers created worms<sup>15</sup> out of curiosity. In the 1980s threat actors (and the U.S. Government) began to realize the exploitation or mayhem that could be inflicted over computer networks. Much of the activity centered on intercepting and decrypting message traffic. The CIA and NSA entered this world as well as the Department of Justice and the Federal Bureau of Investigation. The Soviet Union was the nation that presented the greatest immediate threat, but China was silently learning, and non-nation state actors (“hacktivists”) and organized crime were also beginning to learn, study, and exploit the rapidly developing internet. Today there are malign actors,<sup>16</sup> many of them,<sup>17</sup> who pursue remote access operations.

30. In 2003 the White House issued the National Strategy to Secure Cyber Space, which prioritized securing our networks and ensuring American freedom of movement through other networks and the cyber environment. People, programs, and resources were assembled to accomplish this strategy. In 2005, the Joint Functional Component Command Network Warfare (JFCC-NW) was established. In my office in the Pentagon, I began accumulating memos and documents concerning cyber security.

31. In and after 2002, my responsibilities included overseeing the pursuit of Al Qaeda members hiding in Yemen. We relied upon remote access to all forms of critical infrastructure, communications networks, emissions, and signatures around the world. Our technology and methods were labor and resource intensive, quite manual, and lacked automation to do this with multiple target tracks simultaneously. For high priority intelligence targets, these remote operations could be done, but not on a scale of tens and hundreds of thousand simultaneous surveillance operations.

---

<sup>15</sup> Norton, <https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html>

<sup>16</sup> Cybercrime Magazine, “The History of Cybercrime And Cybersecurity, 1940 – 2020”, November 30, 2020; <https://cybersecurityventures.com/the-history-of-cybercrime-and-cybersecurity-1940-2020/>

<sup>17</sup> Center for Strategic and International Studies, “Significant Cyber Incidents”; <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incident>

32. As time passed, capabilities increased. It was an iterative learning process, with a dizzying exponential increase in “points of presence” (where information was gathered from) and simultaneous remote access operations.

33. The intent of remote access operations was to establish full spectrum dominance of all forms of communication, information technology, and cyber in and around Iraq to project effects. Were these effects used to influence elections? According to a Foreign Affairs article,<sup>18</sup> it was discussed but ultimately not implemented according to those interviewed. The wording in the article implies in my opinion a declination of President Bush to approve a covert finding for the CIA to directly engage on the election and perhaps the direct method of manipulating vote tallies.

34. As time went on in Iraq and chaotic civil war broke out among several factions, we attempted different lines of effort to help establish civil society. Part of this was efficiently generating and delivering cyber effects into Iraq and relevant areas outside of Iraq. General Stan McChrystal, who was now with the Joint Special Operations Command, refined the art form of integrating Remote Access Operations to directly support his Commander’s objectives.

35. I was working as both a Joint Staff J-5 Middle East Staff Officer and an Office of the Secretary of Defense Senior Civilian involved in the deliberations to develop and approve the Executive Order for Countering the Adversary Use of the Internet.<sup>19</sup> These efforts encapsulated the operational and directive authority for a family of worldwide remote access operations as well as what would become PPD-20,<sup>20</sup> a follow on authority for the use of remote access operations which, in theory made the

---

<sup>18</sup> Foreign Affairs, “When the CIA Interferes in Foreign Elections A Modern-Day History of American Covert Action” June 21, 2020

<sup>19</sup> Committee on Armed Services, U.S. Senate, “Foreign Cyber Threats to the United States”, January 5, 2017; [https://irp.fas.org/congress/2017\\_hr/cyber-threats.pdf](https://irp.fas.org/congress/2017_hr/cyber-threats.pdf)

<sup>20</sup> Executive Office of the President, “Fact Sheet on Presidential Policy Directive 20”, January 2013; <https://irp.fas.org/offdocs/ppd/ppd-20-fs.pdf>

authority and approval of remote access more agile and responsive to a greater spectrum of senior leaders.

1  
2 36. A culture of remote access capabilities has now become ubiquitous and perhaps commoditized,  
3 with former government employees alleged to be making use of the same techniques and tools in  
4 private activities after leaving government service. What was nurtured in classified environments has  
5 escaped, one way or another, into the wild.<sup>21</sup>

6 37. There is also distinct mimicry of American methods by foreign governments including China,  
7 Russia, Iran, and Venezuela. During my almost 40 years of experience, the phenomenon has recurred –  
8 we lead and innovate, our competitors then copy us. A computer virus called Stuxnet was planted by  
9 someone into the Iranian nuclear environment, and Agent BTZ was planted right back onto U.S.  
10 Government networks in a seemingly copycat attack, leveraging very similar techniques. The Chinese  
11 Communist government especially, fastidiously, and laboriously studies and analyzes everything,  
12 everything we say and do. If we possibly used remote access operations to enter critical infrastructure  
13 and influence events, the Chinese surely studied our efforts and applied these same capabilities and  
14 strategies. Starting with China’s relentless intellectual property theft in the 1990s and Russia’s cyber  
15 aggression against Estonia in 2007, these governments have used remote access operation tactics,  
16 techniques, and procedures they often watched, studied, and learned from us.

17  
18 38. The U.S launched a Comprehensive National Cybersecurity Initiative (CNCI)<sup>22</sup> in 2008, as  
19 described in the Presidential Directive attached hereto as Exhibit A.  
20  
21  
22

---

23 <sup>21</sup> Atlantic Council, “Surveillance Technology at the Fair: Proliferation of Cyber Capabilities in  
24 International Arms Markets”, November 8, 2021; <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/surveillance-technology-at-the-fair/>

25 <sup>22</sup> FAS.ORG; De-classified Text of HS/NSPD-54/23: Cybersecurity Policy;  
26 <https://irp.fas.org/offdocs/nspd/nspd-54.pdf>

1 39. CNCI included the development of significant new remote access capabilities. Portions of  
2 paragraph 47 of the CNCI document (pages 12-13) are partially redacted and possibly point to  
3 additional capabilities. The CNCI effort was a disruptive, historical inflection point for collection of  
4 information on a massive scale never seen before. From 2007 forward, the ability to penetrate  
5 networks, and manipulate or gain information on scale, expanded exponentially. Robust remote access  
6 operations can range across several functional activities and can possibly include exfiltration or  
7 manipulation of data on a large scale of critical infrastructure—including electronic voting systems.

8 40. There were 12 publicly announced initiatives in the CNCI program. I was a key player in the  
9 de-classification of the 12 CNCI initiatives. It was my job from 2007 – 2014 to act as the senior DoD  
10 lead working in conjunction with OMB, the DNI, DHS, and the DOJ to ensure these CNCI funds were  
11 properly deployed, obligated, implemented, and effectiveness measured.

12 41. Behind the veil of the 12 announced CNCI initiatives, other capabilities lurked involving big  
13 data collection, sorting, and analysis on a scale never before seen—capabilities now seen as routine  
14 with Amazon and Google search. An unprecedented ability emerged to access, exfiltrate, analyze, and  
15 change information in critical infrastructure, which includes electronic election systems. Foreign  
16 governments have once again, studied, and replicated these efforts.

17 42. While significant people, programs, and resources were being generated by CNCI, the Chinese  
18 government conducted a massive remote access penetration and exfiltration operation focused on the  
19 U.S. federal Office of Personnel Management. The operation yielded massive amounts of information  
20 and illustrated how American critical infrastructure involving electronic systems can be penetrated  
21 through remote access operations.

22 43. The OPM breach demonstrated the ease with which a foreign government could access a U.S.  
23 Government “trusted” critical infrastructure network, install enabling malware, and exfiltrate data on a  
24 massive scale. CNN reported 21.5 million Americans were exposed in this breach which started,  
25

perhaps around 2013, just as CNCI was hitting full operational capability. The crown jewel of this massive theft through remote access was hundreds of thousands or more SF-86's —the key U.S. Government form that comprehensively documents a person's history and background for those seeking or renewing a security clearance. These files contained expansive details about everyone who has or had security clearances. There is no reason to believe that our electronic election systems infrastructure could not be similarly penetrated and manipulated.

44. Another example of a nation state using remote access operations to penetrate a critical infrastructure network is the more recent SolarWinds breach, in which enabling malware was planted into software updates which created broad and pervasive presence through many customer networks using Solar Winds Orion software. SolarWinds showed the relative ease of cybersecurity offense penetrating the defense and spreading broadly, perhaps for years, and establishing a decisive position to monitor, surveil, steal, and manipulate data. This breach also illustrates how thousands of systems can be hacked in a coordinated fashion, and shows how the belief that our electronic voting systems are more secure by being purportedly decentralized is a false notion.

45. From about 2008 – 2014, I was one of a small group of inter-agency players involved in a group called the CRG. The purpose of this group was to work the hardest problem set of weaknesses of the American cyber critical infrastructure to foreign remote access operations and turn these into opportunities for American counter moves back into the threat environment to hold our adversaries at risk. In approximately 2014, because of shifting priorities, I no longer attended the CRG meetings, but I often heard updates of their work in in regular internal cyber coordination meetings. In 2016, references to Russian and Chinese interference into the American election process began. The references identified their intrusions into campaign networks. Iran was also a regular threat nation identified.

### Cybersecurity Weakness in U.S. Elections

1 46. In all my election work in U.S. elections, in Bosnia, in Iraq, and in assessment of Taiwan  
2 elections the principles of the Carter Center for Democracy, and their recommended best practices for  
3 free and fair elections, have served as the guideposts. The Carter Center Manual, Chapters 8 – 10,<sup>23</sup> is  
4 considered the gold standard in the conduct of democratic elections. In my professional opinion,  
5 American elections deviate substantively from the best practices endorsed by the Carter Center with  
6 respect to cybersecurity.

7 47. The Carter Center mandates review of electronic voting technologies by an independent body  
8 (P.152). There is no pervasive implementation of qualified independent bodies provided with uniform  
9 minimum standards at the county or state level to review election technologies that I am aware of.  
10 Currently, county election personnel rely entirely on their contractors for administration of election  
11 technologies. I have never come across a county where the sworn election officials know how to  
12 access or see network activity beyond the operator level of any election machine or related information  
13 technology component. There is no independent, third-party verification and validation I have ever  
14 come across. Contractors often assert intellectual property rights or contractual terms and conditions to  
15 deny any third-party review of the network/cloud environment beyond the election machine. For  
16 example, it has been publicly reported that “a software update [was] installed to address a glitch in  
17 Georgia’s voting machines” just a few weeks prior to the November 2020 election.<sup>24</sup> It does not appear  
18 that this “update,” and its purpose or effect, was ever reviewed by any qualified independent bodies.  
19  
20  
21  
22

---

23 <sup>23</sup> The Carter Center, “Election Obligations and Standards”;

24 <https://www.cartercenter.org/resources/pdfs/peace/democracy/cc-OES-handbook-10172014.pdf>

25 <sup>24</sup> AP News, “With time short, judge mulls Georgia voting system changes”, October 7, 2020,  
26 <https://apnews.com/article/technology-senate-elections-georgia-elections-voting-machines-6a6be19f168a719e68c107c7426df9f3>



48. In my professional experience, there often is a monoculture of singular narratives in the national security world that are established and once established are rarely, if ever questioned, challenged, or further investigated. I have experienced this mentality in countless senior level meetings within the Pentagon, the Inter-Agency, and the White House. This strong conformance to a singular narrative incorporated outright hostility to any notion that China interfered in the November 2020 election. On January 7, 2021, the Director of National Intelligence concluded in an unclassified memorandum that “CIA Management took actions ‘pressuring [analysts] to withdraw their support’ for findings regarding China’s actions to “interfere” in the election.<sup>25</sup> The DNI concluded that the CIA’s actions violated Intelligence Community Tradecraft Standards.

#### **Failure of the U.S. Government to Secure the American Election Environment**

49. Recent assertions by federal government officials on the security of U.S. election critical infrastructure against remote access operations are misguided, in my opinion. While these leaders and personnel are of high caliber and well meaning, they simply do not understand the election system, process, nor equipment.

50. Around the November 2020 election, representatives of CISA, including Chris Krebs, Director of CISA, made strong assertions of election security such as “[t]he November 3rd election was the most secure in American history.” In my professional opinion, such statements are false because, in my observations and decades of experience within government, the U.S. Government does not have the people, programs, or resources to have a comment on the true resilience and security of the election critical infrastructure.

---

<sup>25</sup> DNI John Ratcliffe Memo, January 7, 2021; Views on Intelligence Community Election Security Analysis; <https://context-cdn.washingtonpost.com/notes/prod/default/documents/6d274110-a84b-4694-96cd-6a902207d2bd/note/733364cf-0afb-412d-a5b4-ab797a8ba154.#page=1>

51. In addition, two things Mr. Krebs did significantly undermined his credibility. First was his tweet on November 18, 2020, where Mr. Krebs backtracked on his previous assertion of that the November 2020 election was secure.



52. The second was Mr. Krebs’s congressional testimony on February 10, 2021,<sup>26</sup> where his statement was replete with comments on the shortage of people, programs, or resources to provide effective cybersecurity of the American election environment. From Mr. Krebs’s statement, it is hard to reconcile his February 10, 2021, statement with the statement he approved from November 12, 2021:

It is hard to overstate the massive scope of the critical infrastructure security and resilience challenge. The levers government has at its disposal to change behaviors, on the other hand, is underwhelmingly small. This leads to three conditions limiting the ability of government and industry to collectively improve critical infrastructure cybersecurity: (1) lack of a deep understanding of what is truly systemically important across the economy, (2) a need for more meaningful methods for operational engagement with industry to address risk; and (3) insufficient funding and investment in security improvements.

---

<sup>26</sup> Christopher C. Krebs Testimony before Committee on Homeland Security, February 10, 2021, <https://docs.house.gov/meetings/HM/HM00/20210210/111152/HHRG-117-HM00-Wstate-KrebsC-20210210.pdf>

53. In my professional experience and opinion, it is of low probability that the national intelligence collection system was specifically looking for Chinese intervention into any election system infrastructure or components. The catastrophic Target Corporation retail store breach demonstrated how a threat actor can remotely obtain access into key information of an enterprise through related but different critical infrastructure such as facility climate control networks. The Target Corporation breach was closely followed and studied within the U.S. Government. It is of note that none other than Chris Krebs identified this capability of remote access through a related system in a 2014 article on the Target Breach.<sup>27</sup>

54. In my professional opinion, assertions by state and federal officials that electronic election systems in our Country are secure from remote access operations have little basis in fact and are false. My opinion is further supported by other computer science experts such as University of Michigan Professor J. Alex Halderman.<sup>28</sup>

55. In my professional experience and opinion, all components of the American election system at all levels, but especially the crucial and foundational county level, including information technology, election machines, network architecture, ballot design and handling and all related matters are for more complicated than necessary and are void of transparency and understandability for the sworn election officer charged with running the entire process. Far greater public trust and confidence as well as significant cost savings can be had by re-introducing manual processes overseen by trusted, sworn election officers.

---

<sup>27</sup> KrebsonSecurity, Target hackers Broke in via HVAC Company, February 14, 2015, <https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/>

<sup>28</sup> Declaration of J. Alex Halderman in support of Motion for Preliminary Injunction, Civil Action No. 1:17-CV-2989-AT stating 16 states using Dominion machines can have votes “stolen” by “nefarious actors” and begging the court unseal his report on these issues to allow CISA to try and fix these vulnerabilities before the 2022 election.

**Strong Indicators of Sophisticated, Automated, and Nation State Level and/or Witting Insider Enablement of Access**

1 56. As I read the Mesa County report from the perspective of my experience in assessing large  
2 breaches, intrusions, and exfiltrations, the techniques, complexity, and sophistication of the events  
3 identified in the report screamed about advanced capabilities, including possibly Artificial Intelligence  
4 and the all-important enablement by what we would call the “witting” insider when assessing major  
5 network intrusions. The unwitting insider being the personality who clicks on a spear phishing link, or  
6 uses simple passwords or stores them, unsecure on documents, or visible in some way. Cameras on  
7 computers can be accessed and often times anything in an office space is visible – including  
8 handwritten passwords on sticky notes. In reviewing the entire Department of Defense and  
9 Intelligence Community environment from 2014 to 2018, we identified that more than 90% of  
10 breaches traced to one of three vulnerabilities: Lack of Two Factor Authentication (2FA); Spear  
11 phishing, or the Insider threat. That 90% doesn’t necessarily include vulnerabilities in firewalls, anti-  
12 virus programs, or operating systems.

14 57. One of the key areas of concern over cyber vulnerability include remote access to the election  
15 machines. Remote access to networks and systems has been built in from almost the beginning of the  
16 information technology age. Even in early operating systems, the need to update software and  
17 firmware was identified, and the intuitive design feature was to create a “backdoor” to remotely assess  
18 system performance, conduct maintenance, and update software/data sets. All of this makes sense  
19 when viewed from cost efficiencies, ease of access, and the operational usage. This capability was  
20 prevalent in the 1990s when I was involved with the first generation of automated, computer based, air  
21 traffic control, and aids to air navigation. However, those intent on conducting mischief and mayhem  
22 also immediately picked up on this functionality that could be flipped into ingress points into the  
23 network environment.

1 58. ES&S has admitted to building in remote access to their machines. As with many remote  
2 access procedures for maintenance, it does not appear this Mesa County access was or is 2FA enabled.  
3 Many remote access procedures have no password, use an obvious common password, or have not  
4 changed the password literally for years or decades over concern of the system crashing if the  
5 password was changed. An inspection of the machines is required by Colorado Election Statute, but  
6 this legal obligation implies that the inspector has an informed understanding of the machines, and a  
7 nominal visual inspection would likely identify the Election Machine modems, which may be able to  
8 operate in a wireless state.

9 59. A Sworn Election Official, knowing the wireless ability of the election machines would further  
10 be led to the intuitive conclusion of securing their wired and wireless environment and would use a  
11 Wireshark or similar tool to detect wireless traffic and conduct forensics to determine what machines  
12 are talking to what networks. All of these activities fall reasonably within the realm of the statute  
13 required "Inspection". Requirement to know these things is commensurate with the complexity of the  
14 equipment being overseen, which begets the question as to why these election machines are so  
15 sophisticated and complex.

16 60. The report also flagged two additional modus operandi that immediately stood out in my mind;  
17 artificial intelligence enabled swapping of data and the insider. On the first issue, although roughly  
18 25,000 ballots to be scanned may be considered a small number, the commensurate data sets identified  
19 in the report imply advanced computing ability to create, maintain, and update this data and the ability  
20 to project it through the network to the right machines. This is above the ability of humans on  
21 keyboard to orchestrate such activity. A human may design the original algorithms, but actual  
22 Artificial Intelligence activities learn and adapt at faster speeds than humans. The report describes  
23 activities that broach areas beyond immediate human enabled activities.  
24  
25  
26

1 61. The Mesa County situation also points to one of the big three reasons identified earlier for  
2 network breaches: The Witting Insider. This is the most dangerous of the three reasons identified  
3 earlier and despite the many stories in media about breaking into computer networks, this is the one  
4 with the highest probability and the one that inflicts the greatest amount of damage. Please think about  
5 the Edward Snowden episode which is still reverberating to this day. The reality is that any  
6 Intelligence Preparation of the Battlefield (IPB) or Operational Preparation of the Environment (OPE)  
7 for military or intelligence operations immediately lays down the greatly desired aspect of leveraging  
8 the knowledge of an insider which often is irreplaceable and frankly, sensitive national security  
9 operations are unexecutable without this insider.

10 62. The factual reality of the need for an insider, points right back at the Election Machine  
11 Company. With Sworn Officials apparently hermetically sealed off from any modicum of knowledge  
12 of how the election machines work (including the EMS systems), the actuality and likelihood of  
13 successful of network enabled placement of new data sets onto the machines could simply not have  
14 been accomplished without a witting, compliant insider. The representatives of the Election Machine  
15 Companies are the logical persons of interest. Furthermore, even if they weren't, their inability to  
16 detect, understand, and report these intuitively suspicious network activities means they are not  
17 compliant to the terms, meaning, spirit, or intent of the contract with the county or Colorado law.

### 18 19 **Intentional Over-Sophistication of Voting Machine Equipment and Processes**

20 63. With the preceding analysis, another intuitive conclusion is drawn. Why is the voting process  
21 so complicated? Also, why are counties spending so much time and resources on an information  
22 technology environment? Has anyone conducted an evaluation of the cost, time, and motion spend on  
23 automated systems versus hand counting of ballots? Any such evaluation must include accounting for  
24 the greater likelihood of unintended outcomes.  
25

64. With the apparent lack of knowledge from the Sworn Officials, there appeared to be no checks  
and balances or quality control measure to detect or measure the magnitude of such errors, deviations,  
or breakdown of processes in Mesa County. Simply put, it is very likely that simple counting by hand  
will be faster, more accurate, and far less expensive than the current process. Yes, from a credit card  
company perspective with billions of daily transactions, advanced, AI enabled, conduct of the network  
makes sense. We should not be fooled by technology. There's a right time and place for advanced  
computing systems, data storage, processing, networks, and cloud instantiations. We need to be  
thoughtful and discerning on which provides better service to our citizenry. The entire precept of  
electronic voting machines needs to be re-visited.

I declare under penalty of the perjury laws of the State of Virginia and the United States that the  
foregoing is true and correct and that this declaration was executed this 25<sup>th</sup> day of May 2022 in  
Woodbridge, Virginia



---

Colonel, USAR (Retired) John R. Mills  
May 25, 2022

# **EXHIBIT A**



TOP SECRET

**THE WHITE HOUSE**  
**WASHINGTON**

January 8, 2008

**NATIONAL SECURITY PRESIDENTIAL DIRECTIVE/NSPD-54**  
**HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD-23**

**Subject: Cybersecurity Policy (U)**

**Purpose**

- (1) This directive establishes United States policy, strategy, guidelines, and implementation actions to secure cyberspace. It strengthens and augments existing policies for protecting the security and privacy of information entrusted to the Federal Government and clarifies roles and responsibilities of Federal agencies relating to cybersecurity. It requires the Federal Government to integrate many of its technical and organizational capabilities in order to better address sophisticated cybersecurity threats and vulnerabilities. (U)
- (2) This directive (a) provides an enduring and comprehensive approach to cybersecurity that anticipates future cyber threats and technologies and involves applying all elements of national power and influence to secure our national interests in cyberspace and (b) directs the collection, analysis, and dissemination of information related to the cyber threat against the United States and describes the missions, functions, operations, and coordination mechanisms of various cyber operational organizations throughout the Federal Government. (U)
- (3) This directive furthers the implementation of the *National Strategy for Homeland Security*, Homeland Security Presidential Directive-5 (HSPD-5) (*Management of Domestic Incidents*), Homeland Security Presidential Directive-7 (HSPD-7) (*Critical Infrastructure Identification, Prioritization, and Protection*), Homeland Security Presidential Directive-8 (HSPD-8) (*National Preparedness*), Executive Order 13434 of May 17, 2007, (*National Security Professional Development*), and (b)(1) OGA  
(S//NF)
- (4) Actions taken pursuant to this directive will improve the Nation's security against the full spectrum of cyber threats and, in particular, the capability of the United States to deter, prevent, detect, characterize, attribute, monitor, interdict, and otherwise protect against unauthorized access to National Security Systems, Federal systems, and private-sector critical infrastructure systems. (S//NF)

TOP SECRET

Reason: 1.4 (c) (d) (e) (g)  
Declassify on: 1/05/2043

Declassified in Part

Authority EPIC v. NSA, FOIA Case # 58987 (06/05/2014)  
By NH NARA, Date 09/11/2014

TOP SECRET

2

### Background

- (5) The electronic information infrastructure of the United States is subject to constant intrusion by adversaries that may include foreign intelligence and military services, organized criminal groups, and terrorists trying to steal sensitive information or damage, degrade, or destroy data, information systems, or the critical infrastructures that depend upon them. Cyber criminals are intent on malicious activity, including the manipulation of stock prices, on-line extortion, and fraud. These activities cost American citizens and businesses tens of billions of dollars each year. Hackers and insiders have penetrated or shut down utilities in countries on at least three continents. Some terrorist groups have established sophisticated on-line presences and may be developing cyber attacks against the United States. (S//NF)
- (6) The United States must maintain unrestricted access to and use of cyberspace for a broad range of national purposes. The expanding use of the Internet poses both opportunities and challenges. The ability to share information rapidly and efficiently has enabled huge gains in private sector productivity, military capabilities, intelligence analysis, and government effectiveness. Conversely, it has created new vulnerabilities that must be addressed in order to safeguard the gains made from greater information sharing. (S//NF)

### Definitions

- (7) In this directive:
- (a) "computer network attack" or "attack" means actions taken through the use of computer networks to disrupt, deny, degrade, manipulate, or destroy computers, computer networks, or information residing in computers and computer networks; (S)
- (b) "computer network exploitation" or "exploit" means actions that enable operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks; (S)
- (c) "counterintelligence" means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorist activities; (U)
- (d) "cyber incident" means any attempted or successful access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality, security, or availability of data, an application, or an information system, without lawful authority; (U)

TOP SECRET

TOP SECRET

3

- (e) “cyber threat investigation” means any actions taken within the United States, consistent with applicable law and Presidential guidance, to determine the identity, location, intent, motivation, capabilities, alliances, funding, or methodologies of one or more cyber threat groups or individuals; (U)
- (f) “cybersecurity” means prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation; (U)
- (g) “cyberspace” means the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries; (U)
- (h) “Federal agencies” means executive agencies as defined in section 105 of title 5, United States Code, and the United States Postal Service, but not the Government Accountability Office; (U)
- (i) “Federal systems” means all Federal Government information systems except for (i) National Security Systems of Federal agencies and (ii) Department of Defense information systems; (U)
- (j) “information security incident” means a “computer security incident” within Federal Government systems (as described in National Institute of Standards and Technology Special Publication 800-61 “Computer Security Incident Handling Guide”) or critical infrastructure systems that is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices; (U)
- (k) “information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information; (U)
- (l) “intrusion” means unauthorized access to a Federal Government or critical infrastructure network, information system, or application; (U)
- (m) “National Security System” means any information system (including any telecommunication system) used or operated by an agency, an agency contractor, or other organization on behalf of an agency, where the function, operation, or use of that system involves (i) intelligence activities, (ii) cryptologic activities related to national security,

TOP SECRET

TOP SECRET

4

(iii) command and control of military forces, (iv) equipment that is an integral part of a weapon or weapon systems, or (v) critical to the direct fulfillment of military or intelligence missions; or is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. This definition excludes any system that is designed to be used for routine administrative and business applications such as payroll, finance, or logistics and personnel management applications; (U)

- (n) (b)(1) OGA (S//NF)
- (o) “secure” means to defend and protect both military and civilian Government-owned networks; (U)
- (p) “State” and “local government” when used in a geographical sense have the meanings ascribed to them in section 2 of the Homeland Security Act of 2002 (section 101 of title 6, United States Code); and (U)
- (q) “US-CERT” means the United States Computer Emergency Readiness Team in the National Cyber Security Division of the Department of Homeland Security (DHS). (U)

Policy

- (8) Federal agencies shall, consistent with this directive, increase efforts to coordinate and enhance the security of their classified and unclassified networks; increase protection of the data on these networks; and improve their capability to deter, detect, prevent, protect against, and respond to threats against information systems and data. (U)
- (9) Federal agencies shall, as required by law, protect the confidentiality, integrity, and availability of information stored, processed, and transmitted on their information systems, and shall ensure the authentication of access to such systems as required. Federal agencies shall take appropriate measures to reduce the risk to these systems and adequately deter, reduce, and limit the loss of information or the operational degradation of information systems that are critical to the national security, national economic security, or public health or safety. (U)
- (10) The Federal Government shall increase efforts with critical infrastructure sectors to enhance the security of their information networks. (U)

TOP SECRET

~~TOP SECRET~~

Policy Coordination

- (11) Consistent with National Security Policy Directive-1 (NSPD-1) (*Organization of the National Security Council System*) and Homeland Security Presidential Directive-1 (HSPD-1) (*Organization and Operation of the Homeland Security Council*), the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism shall be responsible to the President for interagency policy coordination on all aspects of cybersecurity. (S)
- (12) The CSC PCC shall ensure ongoing coordination of the U.S. Government policies, strategies, and initiatives related to cybersecurity; shall monitor actions to implement this directive; and shall keep informed the Assistants to the President referenced in paragraph 11 of this directive. (U)
- (13) The National Cyber Response Coordination Group (NCRCG) consists of senior representatives from Federal agencies that have roles and responsibilities related to preventing, investigating, defending against, responding to, mitigating, and assisting in the recovery from cyber incidents and attacks. In the event of a cyber incident, the NCRCG will convene to harmonize operational response efforts and facilitate information sharing consistent with HSPD-5 and the National Response Framework. The NCRCG shall provide advice to the CSC PCC, as appropriate. (U)

Roles and Responsibilities

(14) (b)(1) OGA  
(TS)

- (15) Unless otherwise directed by the President with respect to particular matters, the Secretary of Homeland Security shall lead the national effort to protect, defend, and reduce vulnerabilities of Federal systems and the Secretary of Defense shall provide support to the Secretary of Homeland Security with respect to such assignment. The Secretary of Homeland Security shall:
  - (a) Manage and oversee, through US-CERT, the external access points, including access to the Internet, for all Federal systems;
  - (b) Provide consolidated intrusion detection, incident analysis, and cyber response capabilities to protect Federal agencies' external access points, including access to the Internet, for all Federal systems;
  - (c) In coordination with the Director of OMB, set minimum operational standards for Federal Government Network Operations Centers (NOCs) and Security Operations Centers

~~TOP SECRET~~

~~TOP SECRET~~

6

(SOCs) that enable DHS, through US-CERT, to direct the operation and defense of external access points, including Internet access points, for all Federal systems, which the Secretary will certify and enforce; and

- (d) Utilize the National Infrastructure Protection Plan process, in accordance with HSPD-7, to disseminate cyber threat, vulnerability, mitigation, and warning information to improve the security and protection of critical infrastructure networks owned or operated by Federal agencies; State, local, and tribal governments; private industry; academia; and international partners. (U)
- (16) The Director of OMB shall:
- (a) Direct, to the extent practicable and consistent with national security, the reduction and consolidation of Federal Government external access points, including Internet access points, for all Federal systems; (U)
  - (b) Annually assess, in coordination with the Secretary of Homeland Security, network security best practices of Federal agencies, recommend changes to policies or architectures that should be applied across the Federal Government, and ensure Federal agencies comply with standards and policies if adopted by the Director; and (U)
  - (c) Within 180 days after the effective date of this directive, draft an implementation plan, in coordination with the Secretary of Homeland Security, for an agency accountability process to ensure compliance with and the maintenance of mandatory network security practices by Federal agencies. (U)
- (17) The Secretary of State, in coordination with the Secretaries of Defense, the Treasury, Commerce, and Homeland Security, the Attorney General, and the DNI, shall work with foreign countries and international organizations on international aspects of cybersecurity. (U)
- (18) The Secretary of Commerce shall prescribe, in accordance with applicable law, information security standards and guidelines for Federal systems. (U)
- (19) The Secretary of Energy, as authorized in the Atomic Energy Act of 1954 (AEA), as amended, shall, after coordination with the Secretary of Defense and the DNI, prescribe information security standards and guidelines pertaining to the processing of restricted data, as defined in the AEA, in all Federal agencies, as appropriate. (U)
- (20) The Secretary of Defense and the DNI shall provide indications and warning information to DHS regarding threats originating or directed from outside the United States. (U)

~~TOP SECRET~~

~~TOP SECRET~~

7

(21) The DNI analyzes and integrates all intelligence possessed or acquired by the U.S. Government pertaining to cybersecurity. The DNI, as the head of the intelligence community and consistent with section 1018 of the Intelligence Reform and Terrorism Prevention Act (Public Law 108-458), shall implement the policies and initiatives set forth in this directive within and throughout the intelligence community through the DNI's statutory budget, tasking, and intelligence information sharing authorities, in order to ensure appropriate resource allocation and integration of all cybersecurity efforts and initiatives within and throughout the intelligence community. (U)

(22)

(b)(1) OGA

(S//NF)

(23) The Secretary of Defense has responsibility for directing the operation and defense of the Department of Defense's information enterprise, including monitoring of malicious activity in its networks. The Secretary of Homeland Security is responsible for protecting Federal systems by supporting information assurance strategies within Federal agencies through the following: compiling and analyzing security incident information across the Federal Government; informing and collaborating with Federal, State, local, tribal agencies, private critical infrastructure sectors, and international partners on threats and vulnerabilities; providing vulnerability mitigation guidance; supporting public and private incident response efforts; and serving as a focal point to protect U.S. cyberspace. (U)

(24) The Secretary of Homeland Security, supported by the Director of US-CERT, and the heads of Sector-Specific Agencies, as defined by and consistent with HSPD-7, shall conduct outreach to the private sector on cybersecurity threat and vulnerability information. (U)

(25) The heads of all Federal agencies, to the extent permitted by law and necessary for the effective implementation of the cybersecurity mission, shall support and collaborate with the Secretary of Homeland Security. Further, all Federal agencies shall align their own network operations and defense capabilities to provide DHS with visibility and insight into the status of their Federal systems and shall respond to DHS direction in areas related to network security, allowing DHS to effectively protect the Federal Government network enterprise. Federal agencies shall continue to execute their responsibilities to protect and defend their networks. (U)

~~TOP SECRET~~

~~TOP SECRET~~

8

Implementation

- (26) The Secretary of Homeland Security shall establish a National Cybersecurity Center ("Center"), headed by a Director, to coordinate and integrate information to secure U.S. cyber networks and systems. To ensure a comprehensive approach to cybersecurity and anticipate future threats, other cyber activities shall inform, enable, and enhance cybersecurity activities as appropriate, and in accordance with the implementation plan described in paragraph 28 of this directive. (S)
- (27) The Secretaries of Defense and Homeland Security, the Attorney General, and the DNI shall collocate at the Center certain representatives from their respective cybersecurity organizations. Other Federal Government cyber organizations [redacted] shall be collocated or virtually connected as appropriate. (TS//NF)
- (28) Not later than 90 days from the date of this directive, the Secretary of Homeland Security, in coordination with the Secretary of Defense, the Attorney General, the Director of OMB, and the DNI, shall, through the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism, submit to me for approval an implementation plan that includes details on how authorities will be applied, a concept of operations, and the allocation of required resources for the Center. (U)
- (29) The Director of the Center shall:
- (a) Be appointed by the Secretary of Homeland Security with the concurrence of the Secretary of Defense, after consultation with the Attorney General and the DNI, and is supervised by the Secretary of Homeland Security; (U)
  - (b) Have coordination authority over the directors of the cybersecurity organizations participating in the Center, which means the Director has the authority to require consultation between the offices, departments, or agencies collocated in or virtually connected to the Center; however, this authority does not allow the Director to compel agreement or to exercise command; rather, it creates a consultative structure; (U)
  - (c) Support the Secretaries of Defense and Homeland Security, the Attorney General, and the DNI in executing their respective cyber missions, including [redacted] and investigation and prosecution of cyber crime; (TS//NF)
  - (d) Ensure that Federal agencies have access to and receive information and intelligence needed to execute their respective cybersecurity missions, consistent with applicable law

~~TOP SECRET~~



TOP SECRET

9

and the need to protect national security; (U)

- (e) Advise within the executive branch on the extent to which the cyber program recommendations and budget proposals of agencies conform to cybersecurity priorities; (U)
  - (f) When appropriate, recommend and facilitate the adoption of common doctrine, planning, and procedures across all cyber mission areas; and (U)
  - (g) Not direct or impede the execution of law enforcement, intelligence, counterintelligence, counterterrorism, [REDACTED] (b)(1) OGA  
[REDACTED] (S/NF)
- (30) Each Federal agency operating or exercising control of a National Security System shall share information about information security incidents, threats, and vulnerabilities with the US-CERT to the extent consistent with standards and guidelines for National Security Systems and the need to protect sources and methods. (U)
- (31) The National Cyber Investigative Joint Task Force (NCIJTF) shall serve as a multi-agency national focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations, with representation from the Central Intelligence Agency (CIA), National Security Agency (NSA), the United States Secret Service (USSS), and other agencies, as appropriate. Under the authority of the Attorney General, the Director of the Federal Bureau of Investigation (FBI) shall be responsible for the operation of the NCIJTF. This authority does not allow the Director of the FBI to direct the operations of other agencies. The Director of the FBI shall ensure that participants share the methodology and, to the extent appropriate, case information related to criminal cyber intrusion investigations among law enforcement organizations represented in the NCIJTF in accordance with paragraphs 32 – 33. (U)
- (32) The Attorney General shall, by March 1, 2008, develop and publish an initial version of the Attorney General Guidelines for the NCIJTF, in coordination with the heads of other executive departments and agencies as appropriate. (U)
- (33) Within 90 days of the date of this directive, the Attorney General shall submit to the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism an operational plan for the NCIJTF. (U)

TOP SECRET

TOP SECRET

10

Comprehensive National Cybersecurity Initiative

- (34) To achieve the goals outlined in this directive, the Federal Government needs an integrated and holistic national approach that builds upon strengths and addresses vulnerabilities in our current cybersecurity practices. This effort shall include the actions directed in paragraphs 35 – 46. (U//FOUO)
- (35) The Director of OMB shall within 90 days of the date of this directive, after consultation with the Secretary of Homeland Security, submit to the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism a detailed plan for the reduction and consolidation by June 30, 2008, of Federal Government external access points, including Internet access points. (U)
- (36) The Secretary of Homeland Security shall accelerate deployment of the Einstein program to all Federal systems and shall, after consultation with the Attorney General, enhance the Einstein program to include full-packet content and protocol signature detection. The Secretary of Homeland Security, in consultation with the Director of OMB, shall deploy such a system across the single network enterprise referenced above and consistent with paragraph 16 (a) of this directive no later than December 31, 2008. (S//NF)
- (37) Within 120 days of the date of this directive, the Secretary of Defense with respect to Department of Defense information systems and the Secretary of Homeland Security with respect to Federal systems, after consultation with the Attorney General, and the Director of OMB, shall develop and submit, through the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism, for my approval an implementation plan to deploy active response sensors across the Federal systems. Such a plan shall also address relevant legal and policy issues of the active response sensor capability. (TS)
- (38) Within 90 days of the date of this directive, the Director of the Office of Science and Technology Policy (OSTP), after consulting the National Science and Technology Council (NSTC) and the DNI, shall within 90 days of the effective date, develop a detailed plan to coordinate classified and unclassified offensive and defensive cyber research. (U//FOUO)
- (39) Within 45 days of the date of this directive, the DNI, in coordination with the Secretaries of Defense and Homeland Security and the Attorney General, shall submit to the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism a detailed plan, including standard operating and notification procedures, to connect the following cyber centers: NCIJTF; NSA/CSS Threat Operations Center; Joint Task Force-Global Network Operations; Defense Cyber Crime Center; US-CERT; and Intelligence Community Incident Response Center. Within 180 days of this directive, these centers shall be

TOP SECRET

TOP SECRET

11

connected as part of the National Cybersecurity Center. (S//NF)

- (40) Within 180 days of the date of this directive, the DNI and the Attorney General shall develop a cyber counterintelligence plan, including required resources, that comprehensively reflects the scope and extent of cyber threats. This plan should be consistent with the *National Counterintelligence Strategy of the United States*. (U//FOUO)
- (41) Within 180 days of the date of this directive, the Secretary of Defense and the DNI shall develop a detailed plan to address the security of Federal Government classified networks, including specific recommended measures that will significantly enhance the protection of these networks from the full spectrum of threats. (S//NF)
- (42) Within 180 days of the date of this directive, the Secretary of Homeland Security, in coordination with the Secretary of Defense, the Director of the Office of Personnel Management, and the Director of the National Science Foundation, shall, within 180 days of the effective date, submit to the Director of the Office of Management and Budget, the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism a report including a strategy and recommendations for prioritizing and redirecting current educational efforts to build a skilled cyber workforce. The report should consider recommendations by such groups as the National Infrastructure Advisory Council, the President's Council of Advisors on Science and Technology, and the National Security Telecommunications Advisory Committee. The report should focus on training the existing cyber workforce in specialized skills and ensuring skilled individuals for future Federal Government employment. (U//FOUO)
- (43) Within 120 days of the effective date of this directive, the Director of the OSTP, after consultation with the NSTC and the DNI, shall develop a plan to expand cyber research and development in high-risk, high-return areas in order to better protect our critical national interests from catastrophic damage and to maintain our technological edge in cyberspace. (U//FOUO)
- (44) Within 270 days of the date of this directive, the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism shall define and develop a comprehensive and coordinated strategy to deter interference and attacks in cyberspace for my approval. (S//NF)
- (45) Within 180 days of the date of this directive, and consistent with the National Infrastructure Protection Plan and National Security Directive 42 (NSD 42) (*National Policy for the Security of National Security Telecommunication and Information Systems*), the Secretaries of Defense and Homeland Security, in coordination with the Secretaries of the Treasury, Energy, and Commerce, the Attorney General, the DNI, and the Administrator of General Services shall develop a

TOP SECRET

~~TOP SECRET~~

12

detailed strategy and implementation plan to better manage and mitigate supply chain vulnerabilities, including specific recommendations to:

- (a) Provide to Federal Government and defense acquisition processes personnel access to all source intelligence community vendor threat information;
  - (b) Reform the Federal Government and defense acquisition processes and policy to enable threat information to be used within acquisition risk-management processes and procurement decisions; and
  - (c) Identify and broadly implement industry global sourcing risk-management standards and best practices, acquisition lifecycle engineering, and test and evaluation risk mitigation techniques. (S)
- (46) Within 180 days of the date of this directive, the Secretary of Homeland Security, in consultation with the heads of other Sector-Specific Agencies as outlined in HSPD-7, and consistent with the National Infrastructure Protection Plan, shall submit, through the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism, for my approval a report detailing policy and resource requirements for improving the protection of privately owned U.S.-critical infrastructure networks. The report shall detail how the Federal Government can partner with the private sector to leverage investment in intrusion protection capabilities and technology, increase awareness about the extent and severity of cyber threats facing critical infrastructure, to enhance real-time cyber situational awareness, and encourage specified levels of intrusion protection for critical information technology infrastructure. (U//FOUO)
- (47) Implementing the Comprehensive National Cybersecurity Initiative will require key enablers in the following key areas to ensure success.
- (a) The DNI, in coordination with, as appropriate, the Secretaries of State, the Treasury, Defense, Commerce, Energy, and Homeland Security, and the Attorney General, and the Director of OMB, shall:
    - (i) Monitor and coordinate the implementation of paragraphs 35 through 47 (the "Comprehensive National Cybersecurity Initiative" or "Initiative") of this directive;
    - (ii) Recommend such actions as the DNI judges necessary to implement the Initiative to:

~~TOP SECRET~~

~~TOP SECRET~~

- (A) the President; and
- (B) the heads of Federal agencies as appropriate, and the Director of the Office of Management and Budget, for action within their respective authorities; and

(iii) Report not less often than quarterly to the President, through the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism, on implementation of the Initiative, together with such recommendations as the DNI deems appropriate. (U)

(b) The Secretary of Homeland Security and the Attorney General shall ensure adequate support for agents, analysts, and technical infrastructure to neutralize, mitigate, and disrupt illegal computer activity domestically. (S)

(c) The Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the DNI, and other heads of Federal agencies as appropriate shall increase predictive, behavioral, information, and trend analyses to better understand and anticipate foreign cyber and technology developments. (S//NF)

(d) (b)(1) OGA  
(S//NF)

(e) (b)(1) OGA  
(S//NF)

(f) (b)(1) OGA  
(TS)

(g) The Secretary of Defense and the DNI shall increase Information Assurance to protect National Security Systems against intrusion and attack by implementing defenses to significantly reduce current malicious activity and enable network defenders to focus more effectively on more sophisticated threats. Additionally, by strengthening enterprise-wide cross-domain capabilities and utilizing strong identity protection, the

~~TOP SECRET~~

~~TOP SECRET~~

14

Federal Government will begin to enable greater information sharing among the key cyber organizations. (U//~~FOUO~~)

- (48) Within 180 days of the date of this directive, the Director of OMB, in coordination with the heads of all executive departments and agencies, shall perform a comprehensive risk assessment for the loss, manipulation, or theft of all data currently residing on Federal government unclassified networks. The assessment should assume that adversaries have the capability and intent to either capture the data or disrupt mission applications residing on unclassified networks. The assessment should recommend a prioritized description of which data and applications should be migrated to more secure networks. (S//NF)
- (49) Within 120 days of the date of this directive, the Secretaries of State, Defense, and Homeland Security, the Attorney General, and the DNI shall submit to the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism a joint plan for the coordination and application of offensive capabilities to defend U.S. information systems. (U//~~FOUO~~)
- (50) Within 120 days of the date of this directive, the Attorney General and the Secretary of Homeland Security, after coordination with the Secretary of Defense and the DNI, shall submit to the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism a plan for the coordination and application of law enforcement capabilities to better support investigations of cyber incidents in United States networks. (U//~~FOUO~~)

Budget

- (51) For all future budgets, the heads of all executive departments and agencies shall submit to the Director of OMB, concurrent with their budget submissions, an integrated budget plan to implement the cybersecurity actions described in this directive, consistent with such instructions as the Director of OMB may provide. (U)

General

- (52) To the extent of any inconsistencies between this directive and the *National Strategy to Secure Cyberspace* (2003), this directive shall govern. (U)
- (53) This directive:
- (a) Shall be implemented consistent with applicable law and the authorities of executive departments and agencies, or heads of such departments and agencies, vested by law

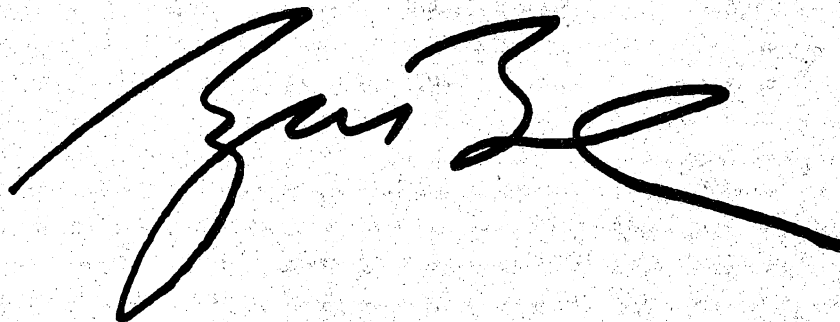
~~TOP SECRET~~

~~TOP SECRET~~

15

(including for the protection of intelligence sources and methods), and subject to the availability of appropriations;

- (b) Shall not be construed to impair or otherwise affect the functions of the Director of OMB relating to budget, administrative, and legislative proposals;
- (c) Shall not be construed to alter, amend, or revoke any other NSPD or HSPD currently in effect;
- (d) Shall not be construed to apply to special activities as defined in section 3.4(h) of Executive Order 12333 of December 4, 1982;
- (e) Shall be implemented in a manner to ensure that the privacy rights and other legal rights of Americans are recognized; and
- (f) Is intended only to improve the internal management of the executive branch of the Federal Government, and is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, against the United States, its departments, agencies, or other entities, its officers or employees, or any other person. (U)

A large, stylized handwritten signature in black ink, appearing to read "Guzik".

~~TOP SECRET~~