The Carter Center

Democracy Program

Human Rights and Election Standards (HRES)

Investigation of the Designation of U.S. Election Infrastructure as Critical Infrastructure Under the Department of Homeland Security

On January 6, 2017, the Office of the Director of National Intelligence released a full report entitled "Assessing Russian Activities in Recent US Elections."[1] On the very same day the Secretary of Homeland Security, Jeh Johnson announced[2] that from then on, election infrastructure shall be designated "Critical Infrastructure" under the 2013 National Infrastructure Protection Plan.[3] These announcements came following intelligence information dating back to the summer of 2016 that entities connected to Russian government had been probing U.S. elections internet-facing infrastructure.[4] This is evidenced in DHS and DNI's joint statement, released in October of 2016, fore-warning state and local election officials to "be vigilant and seek cybersecurity assistance from DHS," and that DHS was working directly with the National Association of Secretaries of State to form an Election Infrastructure Cybersecurity Working Group.[5]

---

[1] https://www.dni.gov/files/documents/ICA_2017_01.pdf

[2] https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical

[3] The NIPP's authorities include the Homeland Security Act of 2002, EO 13636, Presidential Policy Directive (PPD) 21, National Institute of Standards and Technology Cybersecurity Framework, Homeland Security Presidential Directive 7: "Critical Infrastructure, Identification, Prioritization, and Protection," and PPD-8: National Preparedness. https://www.dhs.gov/sites/default/files/publications/NIPP-Fact-Sheet-508.pdf

[4] **6/21/17** Written testimony of I&A Cyber Division Acting Director Dr. Samuel Liles, and NPPD Acting Deputy Under Secretary for Cybersecurity and Communications Jeanette Manfra for a Senate Select Committee on Intelligence hearing titled "Russian Interference in the 2016 U.S. Elections." https://www.dhs.gov/news/2017/06/21/written-testimony-ia-cyber-division-acting-director-dr-samuel-liles-and-nppd-acting

[5] https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national

In a written testimony released on June 21, 2017 presented to a Senate Select Committee on Intelligence hearing titled, “Russian Interference in the 2016 U.S. Elections,” the timeline of this intelligence was revealed. This testimony states that throughout early 2016, “the U.S. IC [Intelligence Community] warned that the Russian Government was responsible for leaks of emails from U.S. political figures…activity was part of a decade-long campaign of cyber-enabled scanning and probing of election-related infrastructure in some states.” This testimony also notes that it was known in October 2016 that internet-facing election-related networks in twenty-one different states had been successfully compromised, though none of the targeted systems involved vote tallying. During this time, it was concluded that due to the diversity and de-centralized nature of U.S. election infrastructure, any cyber activity aimed at changing the outcome of a national election would not only need a multiyear effort with “significant human and information technology resources available only to a nation-state”, but that any such attempt would most certainly be detected. Rather, it was determined that such breaches were intended to “undermine public confidence in electoral processes and potentially the outcome.”

Nonetheless, this intelligence certainly raised alarm, and pointed to an increasing need in an increasingly digitized world, to protect the integrity and independence of U.S. democratic structures, including election infrastructure; hence, the January designation of this infrastructure as “critical.”

This designation means that election infrastructure will become a subsector of the “Government Facilities” critical infrastructure sector under the NIPP. Currently, there are sixteen critical infrastructure sectors and twenty sub-sectors. Each sector is assigned a federal agency known as a Sector-Specific Agency (SSA) that will then be tasked with creating a Sector-

Specific Plan (SSP) to structure and manage the sector.[6] The Election Assistance Commission (EAC) has publicly called on DHS to make it the Co-SSA for this particular sector, given the knowledge gap within DHS about specific operations in the elections sector. Besides the SSA and Co-SSA, other roles need to be filled following a new sector or sub-sector creation. These are a Sector Coordinating Council (SCC) and a Government Coordinating Council (GCC). The former is comprised of private entity stakeholder representatives, "who interact on a wide range of sector-specific strategies, policies, activities, and issues." SCCs are meant to connect government and private sector-specific stake-holders for policy coordination. GCCs are comprised of representatives from all levels of government to facilitate intergovernmental, interagency, and cross-jurisdictional coordination.[7] Furthermore, Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs) must be established to ensure strong lines of communication between all of the afore-mentioned parties. ISACs are responsible for gathering, analyzing, properly sanitizing, and disseminating intelligence to all the stakeholders in their specific sector. They offer 24/7 threat warning and incident reporting. ISAOs are more informal entities, responsible for voluntarily issuing information to its self-organized members and communities of interest. These members can gain access to this de-sensitized information regardless of clearance or knowledge level.[8]

Despite concerns that the Trump Administration would disrupt this process, The Election Infrastructure Cybersecurity Working Group (announced in Secretary Johnson's joint statement in October 2016) met at least twice in 2017, before coalescing into a formal GCC. These

---

[6] pg. 2, EAC, "Starting Point: U.S. Election Systems as Critical Infrastructure." https://www.eac.gov/assets/1/6/starting_point_us_election_systems_as_Critical_Infrastructure.pdf

[7] pg. 2, EAC, "Starting Point: U.S. Election Systems as Critical Infrastructure."

[8] pg. 3, EAC, "Starting Point: U.S. Election Systems as Critical Infrastructure."

meetings occurred on July 27th[9] and August 21st, in Albany, NY and Orange Co., California, respectively. These meetings focused on creating the subsector partnership framework "to include national strategic objectives, governance guidance, information sharing protocols and other related partnership objectives."[10] On August 23rd, a preliminary SCC listening session was held to brief and garner feedback from the non-governmental partners involved in the election infrastructure sub-sector. EAC Chairman Matthew Masterson has said about the meetings, "'As elections continue to take place across the nation and election officials prepare for the 2018 federal election, it is imperative for there to be a means for the nation's election officials to receive actionable information and intelligence regarding the security of their election systems.'"[11]

This imperative was emphasized when news broke on September 22, 2017 that DHS had finally contacted election officials in twenty-one states to inform them of the nature of the security breaches observed, in some cases, over a year earlier.[12] The extreme delay in this disclosure angered many Secretaries of State and reduced confidence the federal government's plan. The deputy undersecretary of the National Protections and Programs Directorate, Bob Kolasky, admitted that the information did not necessarily make it to the right parties at the right time, but that the new working group is going to remedy these gaps in communication.[13] Moreover, some state and local election officials fear that the designation will bring federal regulation of election processes. However, it has been repeatedly emphasized that this

---

[9] https://www.eac.gov/news/2017/07/27/eac-meeting-moves-election-cybersecurity-protections-forward/
[10] https://www.eac.gov/news/2017/09/01/election-critical-infrastructure-subsector-plans-progress-during-recent-meetings/
[11] https://www.eac.gov/news/2017/09/01/election-critical-infrastructure-subsector-plans-progress-during-recent-meetings/
[12] https://www.npr.org/2017/09/22/552956517/ten-months-after-election-day-feds-tell-states-more-about-russian-hacking
[13] http://thehill.com/policy/cybersecurity/358710-homeland-security-cyber-unit-on-alert-for-election-day

designation only intends to streamline communication between key stakeholders and enable DHS to prioritize cybersecurity assets, giving resources to state a local election officials who request it.[14]

The first official GCC meeting was held on October 14th, 2017 in Atlanta, GA. The GCC is comprised of twenty-seven members, three of which are federal government representatives, and the remainder of which are state and local elections representatives.[15] The outcome of this meeting indicates that DHS has partnered with The Multi-State Information Sharing and Analysis Center, the National Association of Secretaries of State and the National Association of State Election Directors to facilitate information sharing among all stakeholders. This meeting also outlined the services provided by DHS and EAC moving forward: "hygiene for internet-facing systems, risk and vulnerability assessments, incident response assistance, information sharing, classified information sharing, file-based cybersecurity advisors and Protective Security Advisors (PSAs), and physical and protective security tools training, and resources."[16]

In a November 29th written testimony detailing the outcome of this first GCC meeting, it is stated that

> …ensuring the integrity of our electoral process is a vital national interest and one of our highest priorities as citizens in a democratic society…As the threat environment evolves, the Department will work with state and local partners to enhance our understanding of the threat; and to provide essential physical and cybersecurity tools and resources available to the public and private sectors to increase security and resiliency.

Both the DHS and EAC websites contain guides detailing this process and resources for stakeholders to increase their cybersecurity awareness and access to DHS security resources.[17]

---

[14] https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical

[15] For a full list of members, please see Appendix A

[16] https://www.dhs.gov/news/2017/11/29/written-testimony-nppd-house-oversight-and-government-reform-subcommittees

[17] Please see Appendix B for a full glossary of terms, provided by the EAC.

Appendix A.

Members of the GCC for the Election Infrastructure Subsector include:

- Lori Augino, Director of Elections, Washington
- Chris H. Chambless, Elections Director, Clay County, Florida
- Judd Choate, Director of Elections, Colorado*
- Jim Condos, Secretary of State, Vermont
- Edgardo Cortes, Commissioner, Virginia Department of Elections
- Bob Giles, Director, Division of Elections, New Jersey
- Mark Goins, Coordinator of Elections, Tennessee
- Ricky Hatch, Clerk/Auditor, Weber County, Utah
- Thomas Hicks, Vice Chairman, U.S. Election Assistance Commission
- Sarah Johnson, City Clerk, Colorado Springs, Colorado
- Neal Kelley, Registrar of Voters, Orange County, California
- Bob Kolasky, Acting Deputy Under Secretary, U.S. Department of Homeland Security*
- Connie Lawson, Secretary of State, Indiana*
- Linda Lamone, Administer of Elections, Maryland State Board of Elections
- Matthew Masterson, Chairman, U.S. Election Assistance Commission*
- Denise Merrill, Secretary of State, Connecticut
- Paul Pate, Secretary of State, Iowa
- Noah Praetz, Director of Elections, Cook County, Illinois*
- Steve Reed, Probate Judge, Montgomery County, Alabama
- Tom Schedler, Secretary of State, Louisiana
- Steve Simon, Secretary of State, Minnesota
- David Stafford, Supervisor of Elections, Escambia County, Florida
- Maggie Toulouse Oliver, Secretary of State, New Mexico
- Todd Valentine, Co-Executive Director, New York State Board of Elections
- Linda von Nessi, Clerk of the Essex County Board of Elections, New Jersey
- Mac Warner, Secretary of State, West Virginia
- Michael Winn, Director of Elections, Travis County, Texas[18]

**GCC Executive Committee Member*

[18] https://www.dhs.gov/news/2017/10/14/dhs-and-partners-convene-first-election-infrastructure-coordinating-council

Appendix B. Glossary[19]

Term	Definition
Critical Infrastructure	Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. (Source:§1016(e) of the USA Patriot Act of 2001 (42 U.S.C. §5195c(e)))
Critical Infrastructure Partnership Advisory Council (CIPAC)	Council established by DHS under 6 U.S.C. §451 to facilitate effective interaction and coordination of critical infrastructure activities among the Federal Government, the private sector, and State, local, tribal and territorial governments. (Source: CIPAC Charter) These meetings are exempt from the Federal Advisory Committee Act (FACA) requirements that they be open to the public and provide meeting materials to the public.
Critical Infrastructure Sector	A logical collection of assets, systems, or networks that provide a common function to the economy, government, or society; NIPP 2013 addresses 16 critical infrastructure sectors, as identified in PPD-21. (Source: NIPP 2013: Partnering for Critical Infrastructure Security and Resilience)
Cybersecurity	The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability; includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and 911 communications systems and control systems. (Source: 2009 NIPP)
Executive Order 13636	Executive Order that calls for the Federal Government to closely coordinate with critical infrastructure owners and operators to improve cybersecurity information sharing; develop a technology-neutral

[19] copied from https://www.eac.gov/election-officials/elections-critical-infrastructure/

	cybersecurity framework; and promote and incentivize the adoption of strong cybersecurity practices. (Executive Order 13636, Improving Critical Infrastructure Cybersecurity, February 2013)/td>
Government Coordinating Council (GCC)	The government counterpart to the Sector Coordinating Council for each sector established to enable interagency and intergovernmental coordination; comprises representatives across various levels of government (Federal and State, local, tribal and territorial) as appropriate to the risk and operational landscape of each sector. (Source: 2009 NIPP)
Information Sharing and Analysis Centers (ISACs)	Operational entities formed by critical infrastructure owners and operators to gather, analyze, appropriately sanitize, and disseminate intelligence and information related to critical infrastructure. ISACs provide 24/7 threat warning and incident reporting capabilities and have the ability to reach and share information within their sectors, between sectors, and among government and private sector stakeholders. (Source: Presidential Decision Directive 63, 1998) ISACs are not operated, controlled, or managed by DHS.
Information Sharing and Analysis Organization (ISAO)	"Any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of gathering and analyzing critical infrastructure information in order to better understand security problems and interdependencies related to critical infrastructure and protected systems, so as to ensure the availability, integrity, and reliability there of; communicating or disclosing critical infrastructure information to help prevent, detect, mitigate, or recover from the effects of a interference, compromise, or a incapacitation problem related to critical infrastructure or protected systems; and voluntarily disseminating critical infrastructure information to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (A) and (B)." (Source: Homeland Security Act of 2002)
Infrastructure	The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole; consistent with the definition in the Homeland Security Act,

	infrastructure includes physical, cyber, and/or human elements. (Source: DHS Lexicon, 2010)
National Annual Report	Each SSA is required to provide an annual report to the Secretary of Homeland Security on their efforts to identify, prioritize, and coordinate CI/KR protection in their respective sectors. (National Infrastructure Protection Plan: The National CI/KR Protection Annual Report)
National Infrastructure Coordinating Center (NICC)	The National Infrastructure Coordinating Center (NICC) is the dedicated 24/7 coordination and information sharing operations center that maintains situational awareness of the nation's critical infrastructure for the federal government. When an incident or event affecting critical infrastructure occurs and requires coordination between the Department of Homeland Security and the owners and operators of our nation's infrastructure, the NICC serves as that information sharing hub to support the security and resilience of these vital assets. (Source: DHS.gov/national-infrastructure-coordinating-center)
National Infrastructure Protection Plan (NIPP)	The National Infrastructure Protection Plan 2013, involving stakeholders from all 16 critical infrastructure sectors, all 50 states, and from all levels of government and industry, provides a clear call to action to leverage partnerships, innovate for risk management, and focus on outcomes, provides an updated approach to critical infrastructure security and resilience, and involves a greater focus on integration of cyber and physical security efforts. (DHS, NIPP Fact Sheet)
National Protection and Programs Directorate (NPPD) – (DHS/NPPD)	[The DHS division] that leads the DHS mission to reduce risk to the Nation's critical physical and cyber infrastructure through partnerships that foster collaboration and interoperability. (Source: DHS FY13 Budget Guidance). NPPD contains the Federal Protective Service, the Office of Identity Management, the Office of Cybersecurity and Communications, the Office of Cyber and Infrastructure Analysis, and the Office of Infrastructure Protection.

Presidential Policy Directive 21 (PPD-21)	[Presidential Directive that] Aims to clarify roles and responsibilities across the Federal Government and establish a more effective partnership with owners and operators and State, local, tribal and territorial entities to enhance the security and resilience of critical infrastructure. (Source: PPD-21, 2013)
Presidential Policy Directive 8 (PPD-8)	[Presidential Directive that] facilitates an integrated, all-of-Nation approach to national preparedness for the threats that pose the greatest risk to the security of the Nation, including acts of terrorism, cyber-attacks, pandemics, and catastrophic natural disasters; directs the Federal Government to develop a national preparedness system to build and improve the capabilities necessary to maintain national preparedness across the five mission areas covered in the PPD: prevention, protection, mitigation, response, and recovery. (Source: PPD-8, 2011)
Protected Critical Infrastructure Information (PCII)	PCII is [information and communications] protected from disclosure. All critical infrastructure information that has been properly submitted and validated pursuant to the Critical Infrastructure Information Act and implementing directive; all information submitted to the PCII Program Office or designee with an express statement is presumed to be PCII until the PCII Program Office determines otherwise. Critical infrastructure information voluntarily shared with the government and validated as PCII by the Department of Homeland Security is protected from, the Freedom of Information Act (FOIA), State, local, tribal, and territorial disclosure laws, use in regulatory actions and use in civil litigation. PCII can only be accessed in accordance with strict safeguarding and handling requirements, and only trained and certified federal, state, and local government employees or contractors may access PCII.(Source: CII Act of 2002, 6 U.S.C. § 131, and www.dhs.gov/pcii-program)
Protective Security Advisors (PSAs)	Trained critical infrastructure protection and vulnerability mitigation subject matter experts who work for DHS and are responsible for ensuring all Office of Infrastructure Protection critical infrastructure security and resilience programs and services are delivered to State, local, tribal, and territorial stakeholders and private sector owners and operator. There are three types: (1) Regional Directors, supervisory PSAs, PSAs, and geospatial analysts. s. (Source: DHS.gov/protective-security-advisors)

Sector Coordinating Council (SCC)	The private sector counterpart to the GCC, these councils are self-organized, self-run, and self-governed organizations that are representative of a spectrum of key stakeholders within a sector. They serve as principal entry points for the government to collaborate with each sector for developing and coordinating a wide range of critical infrastructure security and resilience activities and issues. (Source: Adapted from the 2009 NIPP)
Sector-Specific Agency (SSA)	A Federal department or agency designated by PPD-21 with responsibility for providing institutional knowledge and specialized expertise, as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the allhazards environment. (Source: PPD-21, 2013)
Sector-Specific Plans (SSP)	Planning documents that complement and tailor application of the National Infrastructure Protection Plan to the specific characteristics and risk landscape of each critical infrastructure sector. SSPs are developed by the SSAs in close collaboration with the SCCs and other sector partners. (Source: Adapted from the 2009 NIPP)