Election Infrastructure Preparedness and Response Planning Group Concept of Operations

Overview

Purpose

This document outlines the coordination of federal government activity in support of the cybersecurity of election infrastructure.[1] In particular, it provides a playbook to guide coordination in response to cyber incidents impacting election infrastructure during the 2016 United States election, so that all elements of the federal government are prepared to respond in a coordinated manner. This playbook is based on Presidential Policy Directive 41 (PPD-41), United States Cyber Incident Coordination[2] and adheres to the established three concurrent lines of effort: threat response; asset response; and intelligence support and related activities. Further, it is aligned with the National Cyber Incident Response Plan and Cyber Unified Coordination Group concept of operations, currently under development.

1 "*Election Infrastructure*" is defined in Annex III, Laws/Policy Governing Federal Response, of this document

2 https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

3 For additional information regarding the laws and policies that govern federal government response to election-related incidents, see Annex III, Laws/Policy Governing Federal Response

Scope

This document establishes the federal response plan for a cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable impact to election infrastructure during the 2016 United States election.

Role of the Federal Government

In almost all potential cases of malicious cyber activity impacting election infrastructure, state, local, tribal, and territorial governments, to include their law enforcement agencies, will have primary jurisdiction to respond. On-scene response efforts of the federal government generally will occur at the behest of the owners and operators of any impacted entities, including state and local officials, who have primary jurisdiction over many different aspects of the electoral process, and have the authorities to respond to cyber incidents affecting their networks and systems.[3]

Consistent with PPD-41, because existing incidents involving election infrastructure have collectively been rated as significant, the Cyber Response Group (CRG) has directed the formation of a Cyber Unified Coordination Group (UCG) to coordinate these activities. The Federal Bureau of Investigation (FBI), the Department of Homeland Security (DHS), and the Cyber Threat Intelligence Integration Center (CTIIC), as the federal lead agencies for threat response, asset response, and intelligence support respectively, are actively engaged in response activities and conducting daily coordination calls to discuss both current response actions and plans for ongoing support for the cybersecurity of national elections. The FBI is conducting law enforcement and national security investigative activity concerning cyber activity directed at election infrastructure; DHS is furnishing technical assistance and ongoing guidance to

affected election infrastructure entities; and CTIIC has facilitated information sharing to build situational threat awareness on actual and potential impacts to election infrastructure.
In furtherance of this ongoing coordination, the National Security Council convened an interagency team from the Department of Justice (DOJ), DHS, FBI, and the Office of the Director of National Intelligence (DNI) to develop this playbook to guide additional federal cybersecurity planning and response efforts leading up to and on Election Day.

Pre-Election Coordination, Planning, and Preparation

Election Infrastructure Cybersecurity Working Group

The Secretary of Homeland Security established an Election Infrastructure Cybersecurity Working Group to convene relevant members of federal and state governments to engage with appropriate election infrastructure stakeholders to explore mechanisms for improving the security and resilience of election infrastructure. The EICWG includes representatives from:

- Department of Homeland Security, National Protection & Programs Directorate (NPPD)
- National Association of Secretaries of State
- State and Local Election Officials
- United States Election Assistance Commission
- National Institute of Standards and Technology
- Department of Justice
- Federal Bureau of Investigation
- Department of Defense Federal Voting Assistance Program

Through the EICWG, DHS provided state and local election officials with a number of products that raised awareness of DHS service offerings and capabilities, including cyber hygiene scanning and Risk and Vulnerability Assessment (offered by the NCCIC National Cybersecurity Assessment and Technical Services team); identified relevant points of contact for headquarters and field-based elements, such as Protective Security Advisors (PSAs) and Cyber Security Advisors (CSAs); promulgated best practices on securing voter registration databases and business continuity planning; and, disseminated an unclassified intelligence assessment on cyber threats and vulnerabilities to election infrastructure.

Response Training to Election Crimes Coordinators (ECC) and District Election Officers (DEO)

All of FBI's Election Crimes Coordinators (ECCs) and the DOJ's District Election Officers (DEOs) attended a three-day seminar on Voter Protection and Election Crime in Columbia, South Carolina. The training covered a variety of topics, including the importance of coordinating with state and local law enforcement and local officials throughout the planning process and setting up an Election Day Working Group with local partners to share information quickly and efficiently in the event of an incident. Additionally, the training included an entire session devoted to cyber events and elections, which impressed upon the ECCs and DEOs the importance of coordinating with the Cyber Task Forces in their respective Divisions to ensure full integration and open channels of communication.
ECCs and DEOs have been encouraged to form Election Day Working Groups with their state and local partners, to include state/local election and law enforcement officials. The DHS PSAs and CSAs have coordinated with the FBI's ECCs, and where appropriate will be collocated with the ECC. ECCs have also

coordinated with their FBI Field Office's Joint Terrorism Task Force (JTTF), Cyber Task Forces (CTF) and Foreign Counterintelligence personnel.

Election Infrastructure Cyber Risk Characterization

The NPPD/Office of Cyber and Infrastructure Analysis (OCIA) prepared an analysis to support DHS efforts to provide technical assistance to State and local governments to mitigate vulnerabilities to election systems. The analysis identifies attributes designed to characterize and compare risk on a State-by-State level. This product focuses on States to provide a starting point for prioritizing outreach and technical assistance efforts; as engagement efforts mature at the State level, some data is available at the county level to prioritize efforts within each State.

Reporting Guidance and Information Coordination

By November 1, 2016, DHS, DOJ, and FBI will develop internal guidance for their headquarters and field-based personnel to specify how information on cyber incidents will flow within their organizations; between FBI, DOJ, and DHS; and to other interagency partners, including CTIIC. This will ensure that information from field personnel is shared quickly and efficiently with headquarters personnel and between threat responders and asset responders to create shared situational awareness of cyber incidents on Election Day. This guidance will be developed in line with the scenarios explained in the "Election Day Operations; Steady State Coordination and Incident Handling Efforts" section of this document.

Communications Planning

The DHS Office of Public Affairs, in coordination with DOJ, FBI, and ODNI, will develop integrated public relations guidance that seeks to maintain public confidence in the electoral system in response to reports of cyber incidents impacting election infrastructure. The public relations guidance developed by these agencies will be fully coordinated before November 1, 2016, with the NSC to ensure that appropriate spokespersons are identified, remarks are fully consistent and joint messages are used in any potential cyber incident. This messaging includes private interactions with affected entities, including their leadership. These public statements should be developed to avoid inadvertently calling into doubt the integrity of the voting process and to avoid negative impacts to voter turnout.

Run-Through

On November 1, 2016 NSC will lead a run-through of election-day operations to test federal communications and coordination processes and resolve any technical or coordination challenges ahead of Election Day.

Election Day Operations

Coordinating Federal Command Centers

FBI National Election Command Post

On National Election Day, November 8, 2016, FBI Headquarters, with the support of representatives from DOJ's National Security Division and Criminal Division, will establish a national monitoring Command Post (CP) at the Strategic Information and Operations Center (SIOC) at the J. Edgar Hoover FBI Building. Subject to Election Day events, the CP will run from 6:00am EST through 12:00am EST. The purpose of the CP is to establish a centralized location to monitor election-related activities, track status reports and significant complaints from FBI Field Offices, identify trends indicative of a coordinated

nationwide effort to disrupt the election process, establish communication with other participating federal agencies, provide guidance to United States Attorney's Offices, FBI Field Offices, and secure necessary authorizations from FBIHQ Executive Management and DOJ's National Security Division and Criminal Division in the event of an FBI response to an election-related event. This CP will serve as a national center to monitor and track Election Day activities both cyber and non-cyber. In the event of an election-related incident requiring a substantial DOJ and FBI response (e.g. violence at polling places, coordinated voter intimidation, or a significant cyber incident), an Incident Command Post will be established by either the local FBI Field Office or the responsible FBI Investigative Division. The Incident Command Post will address the situations within their respective areas of responsibility and keep the national CP apprised of significant developments and outcomes.

FBI Cyber Division National Election Day Cyber Incident Command Center

To have the ability to quickly and effectively intake and triage cyber-related events on Election Day, the FBI Cyber Division will activate enhanced coordination procedures and stand up the FBI's National Election Day Cyber Incident Command Center co-located with CyWatch at the National Cyber Investigative Joint Task Force (NCIJTF). This preparation step will allow the FBI to respond immediately and coordinate any cyber incident related information, eliminating the time needed to re-constitute resources that would need to be applied for significant level events. It also will provide a mechanism to share information with DHS via the NCCIC to aid its response efforts. The FBI's CICC will be activated on Monday November 7 2016, during regular business hours, and on Election Day, Tuesday, November 8 2016, from 6:00am EST through 12:00am EST.

National Cybersecurity and Communications Integration Center (NCCIC)

To quickly and effectively intake and triage cyber-related events on Election Day that may be reported to the NCCIC by FBI through the National Election Day Command Post or the National Election Day Cyber Incident Command Center or received directly by NCCIC via state and local officials or NPPD field-based personnel, the NCCIC will augment its normal operations on Election Day with additional watch officers and incident management personnel at its headquarters facility in the National Capital Region. This will enable the NCCIC and FBI to respond immediately to coordinate any cyber incident and reduce the time needed to activate additional resources to support a significant cyber event.

Cyber Threat Intelligence Integration Center (CTIIC)

CTIIC will operate on Election Day, Tuesday, November 8, 2016, from 0600 through 2400 hours. Leading up to and on Election Day, CTIIC will work with the Intelligence Community and UCG partners to aggregate relevant intelligence and information to build and maintain a common threat and incident picture that informs decision-making. This common picture will set cyber incidents in the context of adversary activity across all domains to draw connections and implications, and will be generated from both serialized reporting and updates on ongoing operations, including actions taken by USG elements to mitigate and defend against identified threats or incidents. CTIIC will facilitate sharing of intelligence on election-related threats and incidents, integrated analysis of election-related threat trends and events, identification of knowledge gaps, and efforts to develop options to degrade or mitigate adversary threat capabilities. In addition to augmenting its normal staff activities on Election Day, CTIIC is coordinating with FBI, NCIJTF, and DHS to co-locate CTIIC personnel with their Command Posts to ensure the timely flow of intelligence and information to all appropriate parties.

Steady State Coordination and Incident Handling Efforts

Based on experience from previous elections as well as heightened awareness of cyber-threats leading up to this election, DHS, DOJ, and FBI anticipate receiving a high volume of incident reporting on Election Day. Interagency response efforts will be based on the relative risk of each cyber incident reported on Election Day, assessed against the cyber incident severity schema. If a cyber incident requires immediate onsite response, DOJ's Criminal and Civil Rights Divisions and FBI Cyber Division will coordinate necessary authorization to conduct investigative activity at or near the polling place, and make sure all interagency components are informed.

All cyber incident reports will be shared amongst DHS, FBI, and CTIIC, whether generated by DHS or FBI field-based personnel centered on information provided by state and local officials and then sent to the NCCIC, CyWatch, or SIOC, or reports directly sent to the NCCIC, CyWatch, or SIOC by elections officials or other state and local partners. Incident information will be shared via the liaison officers and personnel DHS, FBI, and CTIIC embed in each other's watch centers and command posts on Election Day and then shared back with their respective organizations.

Leveraging the DHS intelligence assessment[4] the interagency anticipates that the vast majority of cyber incidents will be assessed as "baseline" or "low" on the schema. These are unsubstantiated or inconsequential events, or events that are unlikely to impact health or safety, national security, economic security, foreign relations, civil liberties, or public confidence. For these incidents, federal response efforts will be limited to maintaining shared situational awareness among DHS, FBI, and the relevant cyber centers, and providing senior leadership in respective departments and agencies and the National Security Council a high level overview of the incidents being tracked at regular intervals. Shared situational awareness includes triaging and deconflicting reporting as it is coming into federal cyber centers, command posts, field-based elements, and state and local partners, such as the MS-ISAC or state and major urban area fusion centers, through regular communication, coordination, and collaboration.

[4] DHS publication titled, *Cyber Threats and Vulnerabilities to US Election Infrastructure*, September 20, 2016

These Coordination calls will be pre-scheduled and will occur throughout the day on Election Day at 0900, 1200, 1500, 1800, 2100, and 2400 hours. Calls will be generated from the FBI's Cyber Incident Command Center, and include NCCIC, CTIIC, and the Cybersecurity Directorate of the National Security Council, at a minimum. During the calls all entities will share relevant threat and incident reporting and make determinations on the severity of cyber incidents, if any occur.

FBI Cyber Division's Major Cyber Crimes Unit (MCCU) will be the lead FBI entity for managing election-related cyber incidents. Personnel from MCCU will be embedded in both the FBI's National Election Command Post and the FBI's Cyber Incident Command Center. MCCU in will be responsible for ensuring that cyber-related reports and complaints are deconflicted and routed through the appropriate FBI Divisions.

Significant Incident Response Efforts

If DHS, DOJ, FBI, and CTIIC assess that a cyber incident on Election Day is (or group of related cyber incidents that together are) likely to result in demonstrable impact to election infrastructure, and be considered a Level 3/Orange or higher according to the U.S. Government Cyber Incident Severity

Schema, DHS, FBI, and CTIIC will activate enhanced procedures and allocate the resources described in their enhanced coordination procedures to coordinate incident response activities. The following resources are available in the event of a significant cyber incident and will be allocated at the discretion of their agency's executive management to respond appropriately.

FBI Response Mechanisms

Cyber Task Forces (CTF)

Cyber Task Forces (CTFs) are located in each of FBI's 56 field offices and bring together federal, state, and local law enforcement entities in each area of responsibility (AOR) to facilitate joint information sharing, incident response, law enforcement, and intelligence actions. In the event of a significant cyber incident, CTFs will be able to quickly respond to affected entities in their respective AORs with concurrence from the local ECC and the FBI's National Election Command Post.

Regional Computer Forensics Laboratory (RCFL)

In the event of a significant cyber incident, cyber forensic personnel are dispersed in field offices and regional computer forensic labs. If digital evidence personnel are needed for large scale deployments, the FBI's Operational Technology Division Emergency planning office will assist.

Cyber Action Team (CAT) Deployments

CAT personnel are located in 26 field offices and one overseas location. Four CAT members have been placed on stand-by and can be deployed immediately if cyber investigative techniques are needed to rapidly respond to a call for assistance or as part of a joint response team. CAT Personnel will not self-deploy to any election related cyber incident on Election Day without coordinating with the local ECC and the FBI's National Election Command Post at SIOC.

FBI Headquarters Surge Capability

FBI Cyber Division's Major Cyber Crimes Unit will be embedded within the FBI's National Election Command Post and the FBI's Cyber Incident Command Center in order to leverage existing analytic and investigative capabilities in the event of a significant incident. Additionally, FBI Cyber Division leadership is prepared to surge headquarters-level resources, dependent on the nature of the incident and the suspected attribution. Major Cyber Crimes Unit will ensure that all relevant FBI Divisions and units are made aware if a cyber incident occurs, and necessary personnel can be brought to either the FBI's National Election Command Post or the FBI's Cyber Incident Command Center to assist.

DHS Response Mechanisms

To fulfill its asset response role and in parallel with the FBI's threat response efforts, DHS, through the NCCIC Hunt and Incident Response team, can provide affected entities onsite or remote assistance, on a voluntary basis. NCCIC activities in support of an affected entity will occur within the incident response lifecycle. This lifecycle includes establishing communications with the entity, triaging the incident and gathering information, developing and implementing a tactical mitigation plan, and post-mitigation information gathering. During the development and implementation of a tactical mitigation plan, NCCIC services and capabilities may include a review of the network or infrastructure of the affected entity, forensics, such as log analysis, hunt analysis, digital media analysis, and malware analysis, a security program and risk review, and finally, recommend mitigations. DHS CSAs and PSAs may also support response efforts.

Post-Election Day Coordination Efforts

Following Election Day, criminal law enforcement investigations will proceed under DOJ and FBI leadership, and agencies will maintain the UCG coordination mechanism until Friday, November 11, 2016 in order to be ready to address any post-election cyber incidents (e.g., planted stories calling into question the results). After this date, the UCG will dissolve, unless members of the CRG agree that is needs to continue operation. DHS, DOJ, FBI, and ODNI will continue their coordination and activities on an as-needed basis to address systematic risks and threats. In particular, the Public Affairs offices of these agencies will stand ready to work with NSC on any public communications concerning any cyber incidents related to the electoral system or in response to any claims or statements made by third parties about any such alleged cyber incidents or activity.

Annex I: Standing Federal Government Organizational Elements

Department of Justice (DOJ)

Headquarters-Based Elements

The Election Crimes Branch

The Election Crimes Branch oversees the Department's handling of all election crime allegations other than those involving federal voting rights, which are handled by the Civil Rights Division. Specifically, the Branch provides advice and guidance on three types of election crime cases: (1) vote frauds, such as vote buying and absentee ballot fraud; (2) campaign-financing crimes, most notably under the Federal Election Campaign Act (FECA); and (3) patronage crimes, such as political shakedowns and misuse of federal programs for political purposes. Vote frauds and campaign-financing offenses are the most significant and most common types of election crimes.

Counterintelligence and Export Control Section

The Counterintelligence and Export Control Section (CES) in the National Security Division (NSD) of DOJ is responsible for investigations and prosecutions affecting, involving, or relating to the intelligence activities of foreign nations, including state-sponsored hacking, espionage, and other violations of federal law.

Computer Crime and Intellectual Property Section

The Computer Crime and Intellectual Property Section (CCIPS) in the Criminal Division of DOJ is responsible for support to investigations and prosecutions involving criminal threats to computer systems. It also provides advice and assistance on electronic evidence collection in criminal matters to agents and prosecutors across the United States.

The Civil Rights Division

The Voting Section of the Civil Rights Division oversees the Department's handling of federal voting rights matters other than the election crimes within the jurisdiction of the Election Crimes Branch and the Criminal Section of the Civil Rights Division. For example, the Voting Section has jurisdiction to investigate and bring legal action to address violations of the Help America Vote Act, which both require a single uniform, official, centralized computerized statewide voter registration list containing registration information for every legally registered voter, and requires that list to be secure against unauthorized access.

Regional-Based Elements

District Election Officers (DEO)

The DEO Program is designed to ensure that each of the Department's 94 United States Attorneys' Offices has a trained prosecutor available to oversee the handling of election crime matters within the district and to coordinate district responses with Department headquarters regarding these matters. The DEO Program involves appointing an Assistant United States Attorney in each federal district to serve a two-year term as a DEO and providing periodic training for the DEOs in the handling of election crime and voting rights matters.

The DEO Program is also a crucial feature of the DOJ's nationwide Election Day Program, which takes place during the federal general elections held in November of even-numbered years. The Election Day Program ensures that federal prosecutors and investigators are available both at Department

headquarters in Washington, DC, and in each district to receive complaints of election irregularities while the polls are open.

Computer Hacking and Intellectual Property (CHIP) coordinators

Consists of over 200 Assistant United States Attorneys in districts across the country, trained in obtaining legal process for investigating criminal attacks on computer systems and networks, and in lawful collection of electronic evidence for prosecutions. Together with the Criminal Division's Computer Crime and Intellectual Property Section, CHIP coordinators address domestic and international criminal activity that affects computer systems.

National Security Cyber Specialist (NSCS) Network

Consists of at least one Assistant United States Attorney in every judicial district and National Security Division attorneys that coordinate the Department of Justice's work to combat cyber threats to the national security, and to work with other components and the United States Attorney's Offices to ensure that the Department takes an all-tools approach to these threats, including by coordinating with the intelligence community on attribution of and response to national security threats.

In the event of an significant cyber event affecting an election, the CHIP and NSCS networks of prosecutors would work with the District Election Officer and FBI investigators to ensure that the investigation of the event is conducted lawfully and appropriately consistent with both the law and policy governing election-related investigations and the law and policy governing the collection of electronic evidence.

Federal Bureau of Investigation (FBI)

Headquarters-Based Elements

Public Corruption and Civil Rights Section (CID/PCU) of the Criminal Division

The Campaign Finance and Ballot Fraud Initiative under PCU is tasked with the mission of strengthening the FBI's ability to address allegations of ballot fraud, voter intimidation, campaign finance violations, and other matters related to elections. The initiative manages the Election Crimes Coordinator Program and provides resource materials, guidance, training, and coordination with DOJ.

Cyber Division (CyD)

FBI Cyber Division's (CyD) mission is to identify, pursue, and defeat cyber adversaries targeting global U.S. interests through collaborative partnerships and FBI's unique combination of national security and law enforcement authorities. CyD manages investigations into computer intrusions targeting the national information infrastructure, Internet-facilitated criminal activity, and supports FBI priorities across program lines, assisting Counterterrorism, Counterintelligence, and Criminal investigations that call for technical expertise. Many of these investigations often have international facets and national economic implications. CyD addresses cyber threats arising from these varied sources in a coordinated manner, allowing the FBI to stay technologically one step ahead of the cyber adversaries threatening the United States. Within Cyber Division, the Major Cyber Crimes Unit under Cyber Operations Section V is responsible for managing election related computer intrusions.

Counterintelligence Division (CD)

The Counterintelligence Division's (CD) mission is to protect the United States by identifying, understanding, and combating foreign government activities which pose a threat to national security. CD, in close collaboration with the Cyber and Criminal Divisions, has established a priority focus to

identify foreign government attempts to influence or disrupt the U.S. presidential election and collection against the new administration. CD will continue to identify lead information for field office investigative efforts. CD, along with CyD, will be issuing a Collection Emphasis Message for field offices with additional guidance.

National Cyber Investigative Joint Task Force (NCIJTF)

The National Cyber Investigative Joint Task Force (NCIJTF) is a multi-agency center that serves as the national focal point for coordinating, integrating, and sharing information related to cyber threat investigations. The task force performs its role through the cooperation and collaboration of its co-located nineteen partner agencies, its four affiliate member agencies, and its on-site representatives from both international partners and state and local law enforcement organizations.

CyWatch is the FBI's 24-hour command center for cyber intrusion prevention and response operations. CyWatch receives threat and incident reporting, assesses it for action, and engages with the appropriate components within Cyber Division, the field, and other agencies for action. The NCIJTF utilizes CyWatch as its 24/7 capability in carrying out its mission of coordinating, integrating, and sharing cyber threat investigation information. Both CyD and its NCIJTF bring a variety of resources to CyWatch to make it the 24/7 focal point for the cyber threat investigations for the nation.

Cyber Action Team (CAT)

The FBI's CAT is a headquarters-managed cadre of highly trained and experienced FBI cyber investigators compromised of specials agents and computer scientists. CAT's mission is to provide a diverse, geographically distributed surge capability of highly-trained personnel for incident response and investigation. CAT resources are deployed when any FBI division identifies a critical need for technical personnel and capabilities that are not present or when local resources are not sufficient to handle a particular situation.

Field-Based Elements

Election Crimes Coordinators (ECC)

ECCs are the lead points of contact in each of the FBI's 56 field offices for election related issues. ECCs are trained with managing all incidents related to elections regardless of the nature of the threat. Each ECC is provided with training and guidance on how to appropriately respond to election incidents and voting issues around the country.

Cyber Task Forces (CTF)

CTFs are organized elements in each of the FBI's 56 field offices that focus on cybersecurity threats. Each CTF conducts cyber threat investigations under the leadership of an FBI cyber squad supervisor and are comprised of special agents, intelligence analysts, computer scientists, other federal agency partners, and state, local, tribal, and territorial law enforcement.

Department of Homeland Security (DHS)

Headquarters-Based Elements

National Cybersecurity and Communications Integration Center (NCCIC)

The NCCIC is a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the federal government, intelligence, community, law enforcement, SLTT governments, and the private sector. The NCCIC shares information

among public and private sector partners to build awareness of vulnerabilities, incidents, and mitigations.

NCCIC Hunt and Incident Response Team (HIRT)

NCCIC's HIRT performs both on-site and remote cyber security incident response. The goal is to discover the malicious actor, acquire/analyze the malicious tools, and mitigate the intrusion. HIRT service offerings include: Incident Triage, Network Topology Review, Infrastructure Configuration Review, Log Analysis, Incident Specific Risk Overview, Hunt Analysis, Security Program Review, Digital Media Analysis, Malware Analysis, and Mitigations.

NCCIC National Cybersecurity Assessment and Technical Services (NCATS)

NCATS offers cybersecurity scanning and testing services that identify vulnerabilities within stakeholder networks and provide risk analysis reports with actionable remediation recommendations. These critical services enable proactive mitigation to exploitable risks and include network mapping and system characterization; vulnerability scanning and validation; threat identification and evaluations; social engineering, application, database, and operating system configuration review; and incident response testing. NCATS technical offerings, to include Cyber Hygiene scanning and on-site Risk and Vulnerability Assessments, are available to state and local election officials on a voluntary, no-cost basis.

Regional-Based Elements

Cyber Security Advisors (CSAs) and Protective Security Advisors (PSAs)

DHS field personnel include Cyber Security Advisors (CSAs) and Protective Security Advisors (PSAs) who provide immediate and sustained assistance, coordination, and outreach to prepare and protect both SLTT and private sector entities from cyber and physical threats. State and major urban area fusion centers are state owned and operated, designated by the governor of each state. They are focal points for the receipt, analysis, gathering, and sharing of threat-related information between federal, SLTT, and private sector partners.

United States Secret Service (USSS)

Headquarters-Based Elements

Criminal Investigative Division (CID)

CID plans, reviews, and coordinates domestic, and domestic and international criminal investigations of USSS, to include those criminal investigations related to malicious cyber activity and cyber incidents, to include potential significant cyber incidents, in accordance with the criminal investigative responsibilities of USSS. Criminal investigative responsibilities of USSS includes conducting investigations of potential violations of 18 U.S.C. §§ 1029 & 1030 and operating a national-network of electronic crimes task forces.

Regional-Based Elements

Electronic Crimes Task Forces (ECTFs)

The Secret Service operates a network of 39 ECTFs, which have the statutory mission to prevent, detect, and investigate various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems. Secret Service ECTFs are a strategic alliance of law enforcement, academia, and the private sector dedicated to confronting and countering cyber threats. Membership in Secret Service ECTFs includes: over 4,000 private sector partners; over 2,500 international, federal, state and local law enforcement partners; and over 350 academic partners.

Cyber Threat Intelligence Integration Center (CTIIC)

Current Intelligence Section (CIS)

CIS is focused on building shared situational awareness of foreign cyber threat intelligence. They produce the Cyber Threat Intelligence Summary, providing timely awareness of significant cyber threat reporting, supplemented with context and analysis.

Analysis Integration Section (AIS)

AIS is tasked with integrating multidisciplinary, all-source analysis of current and near term foreign cyber threats and incidents. They produce assessments with an integrated view of cyber threat issues.

Threat Opportunity Section (TOS)

TOS facilitates and supports interagency efforts to develop and implement coordinated plans to counter foreign cyber threats to US national interests.

Department of Defense (DOD)

Headquarters and Regional-Based Elements

The Department of Defense (DOD) may support civil authorities in response to cyber incidents based upon a request from a federal agency, and the direction of the Secretary of Defense or the President. Support may be provided based on the needs of the incident, the capabilities required, and the readiness of available forces. Available forces for incident response in a federal status could include the Active and Reserve Components, to include National Guard.

Annex II: State and Local Government Entities

Secretaries of State

In most states, the Secretary of State or Secretary of the Commonwealth is the chief administrative position in the state government. This position typically supervises record keeping and thus is usually the chief election official for the state or commonwealth.

State Election Directors

The state election director is the public administrator responsible for managing elections, usually answering to the Secretary of State.

Local Election Officials

Local election officials manage the voting process itself. Depending on state or territorial law, they may be responsible for election implementation, or they may take direction from the state election director.

Homeland Security Advisors

Homeland security advisors are state or territorial positions focused on homeland security. Homeland security advisors may coordinate state participation in federal homeland security activities, develop emergency preparedness policies and procedures, and advise the governor on homeland security policies and priorities.

National Association of Secretaries of State (NASS)

NASS is the professional organization for Secretaries of State and equivalent positions. Key initiatives support elections and voting and state business services, reflecting the varied record management responsibilities held by these positions.

National Association of State Election Directors (NASED)
NASED is the membership association for State Election Directors. NASED's mission is to promote accessible, accurate and transparent elections within US jurisdictions. The association serves as a forum in which to share best practices, bringing together election officials from 55 states and territories for biannual conferences.
State and Major Urban Area Fusion Centers
Fusion centers operate as state and major urban area focal points for the receipt, analysis, gathering, and sharing of threat-related information between federal, SLTT, and private sector partners. DHS Intelligence and Analysis deploys field personnel to fusion centers as Intelligence Officers, Reports Officers, and Regional Directors to foster information sharing between all homeland security stakeholders.
Elections Assistance Commission (EAC)
The EAC is a federal agency tasked with providing information for U.S. election officials pursuant to the Help America Vote Act of 2002 (HAVA). The EAC develops guidance and procedures to comply with HAVA requirements, including adopting voting systems guidelines and certifying voting systems. EAC is led by three presidentially-appointed EAC commissioners. One of the main functions of the EAC is to provide assistance to election officials and helping to coordinate information sharing efforts so that all jurisdictions have access to the same resources.
Multi-State Information and Sharing Analysis Center (MS-ISAC)
The MS-ISAC is a key resource for cyber threat prevention, protection, response, and recovery for the Nation's SLTT governments. It operates a 24/2 Security Operations Center, which provides real-time network monitoring, dissemination of early cyber threat warnings, and vulnerability identification and mitigation to reduce cyber risks to SLTT governments.
National Guard
Every State has the option of utilizing its internal National Guard cyber capabilities in support of state government or civil authorities in a State Active Duty Status under the authority of the Governor.

Annex III: Laws/Policy Governing Federal Response

Federal Government Jurisdiction

States have the primary responsibility for conducting elections, including those that involve the election of federal candidates. However, Congress has provided by a variety of statutes for a federal role in ensuring voter access to the polls and the integrity of electoral systems (e.g., 52 U.S.C. § 21083(a)(3), which, through civil remedies, requires state and local officials to provide adequate technological security measures to prevent unauthorized access to computerized statewide voter registration lists).

Prohibition of Staging Armed Federal Personnel at Polling Places

Pursuant to 18 U.S.C. § 592, armed federal personnel, including federal law enforcement agents, are restricted in responding to an active polling place in an operational capacity. An armed federal response to an active polling place may create felony liability for the responsible federal officials or employees. Armed federal personnel, however, may be present at an active polling place in their personal capacity to cast their own votes.

It is important to note that the Department of Justice has concluded that armed federal law enforcement agents may, where otherwise appropriate, respond to a cyber or other incident at a polling place that has caused it to cease functioning (i.e. when balloting has entirely ceased at that location).

Federal jurisdiction over election felonies exists under the following statutes, among others, that might likely be applied to various forms of malicious cyber incidents on the electoral process or supporting infrastructure:

- **18 U.S.C. § 241:** Conspiracy by any two or more persons to violate any federal right.
- **18 U.S.C. § 245:** Using 'force' to interfere with voting or qualifying to vote, qualifying or campaigning as a candidate, or qualifying of serving as an election official. (Note: Department of Justice policy requires high-level approval to use this statute.)
- **18 U.S.C. § 1030(a) (2):** Accessing information in excess of authorization or without authorization (e.g. theft of registration information).
- **18 U.S.C. § 1030(a) (5):** Damaging computer systems (e.g. electronic voting machines or vote tabulation computers).
- **52 U.S.C. § 10307(c):** Giving false information as to name, address or period of residence in the voting district for the purpose of establishing eligibility to register or vote, or conspiracy to encourage false registration or illegal voting with a federal candidate on the ballot.
- **52 U.S.C. § 20511:** Where there is a federal candidate on the ballot, attempting to deprive or defraud the residents of a State of a fair and impartially conducted election process, by procurement or submission of voter registration applications that are known to be materially false, fictitious, or fraudulent under the laws of the State; or procurement, casting, or tabulation of ballots that are known to be materially false, fictitious, or fraudulent under the laws of the State.
- **52 U.S.C. § 10307(e):** Voting more than once with a federal candidate on the ballot.

Department of Justice policy controls the nature and timing of investigations and charges in election crime cases. Specifically, it is the policy of the Department of Justice to ensure that criminal investigations do not interfere with the State and local administration of elections. The Department of Justice has long maintained that federal criminal law does not have a role in determining which candidate won a particular election, or whether another election should be held because of election misconduct.[5] Likewise, it is Department of Justice policy to constrain both its overt investigative activity and the timing of any charges so as not to potentially affect any ongoing election. Accordingly, overt criminal investigative measures should not ordinarily be taken until the election process is concluded and the results certified.[6] Any exception requires consultation within the Department of Justice.

[5] *Federal Prosecution of Election Offenses*, p. 93 (7th Ed. 2007).
[6] *Id.* at 94.

Election Infrastructure

Elections involve a diverse set of assets, systems, and networks, both public and private. Based on analysis of each phase of the election process, DHS assesses that the following election infrastructure

represent the physical and cyber assets, systems, and networks most critical to the security and resilience of the election process:

- Storage facilities, which may be located on public or private property that may be used to store election and voting system infrastructure before Election Day.
- Polling places (including early voting locations), which may be physically located on public or private property, and may face physical and cyber threats to their normal operations on Election Day.
- Centralized vote tabulation locations, which are used by some States and localities to process absentee and Election Day voting materials.
- Information technology infrastructure and systems used to maintain voter registration databases.
- Voting systems and associated infrastructure, which are generally held in storage but are located at polling places during early voting and on Election Day.
- Information technology infrastructure and systems used to manage elections, which may include systems that count, audit, and display election results on election night on behalf of State governments, as well as for postelection reporting used to certify and validate results.

This planning document focuses on incidents affecting the cyber assets, systems, and networks of election infrastructure and not the physical assets.