



Patel Patriot

## Part 5 - The Cybersecurity Infrastructure Security Agency & Dominion Voting Systems

### Critical Infrastructure

President Harry Truman created the National Security Council (NSC) in 1947. Since its founding, every president has issued some form of national security directives. National security directives are usually directed only to the NSC and senior executive branch officials and lay out foreign and military policy-making guidance. Bill Clinton's Presidential directive PDD-63 of May 1998 started including extensive **critical infrastructure protection (CIP)**. PDD-63 mandated the formation of a national strategy for CIP.

In the wake of the September 11th terrorist attacks, numerous changes took place regarding how we define and operate our CIP. The Patriot Act was signed into law on October 26th, 2001 and gave the following definition for critical infrastructure:

(e) **CRITICAL INFRASTRUCTURE DEFINED.**—In this section, the term “critical infrastructure” means 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.

The following year (November 25, 2002), the Homeland Security Act was signed into law creating the United States Department of Homeland Security. In 2003, President George W. Bush signed the Homeland Security Presidential Directive 7 (HSPD-7) which replaced PDD-63 and established the U.S. National Policy for identification of and prioritization of critical infrastructure. HSPD-7 called for The National Infrastructure Protection Plan (NIPP) which aims to unify Critical Infrastructure and Key Resource (CI/KR) protection efforts across the country. The NIPP's goals are to protect critical infrastructure and key resources and ensure resiliency. It was not an actual plan to be carried out in an emergency, but it was **useful as a mechanism for developing coordination between government and the private sector.**

The NIPP is structured to create partnerships between Government Coordinating Councils (GCC) from the public sector and **Sector Coordinating Councils (SCC) from the private sector.** I want to again emphasize that the SCCs are from the private sector.

Here is the [National Infrastructure Protection Plan \(fas.org\)](https://fas.org)

Protecting the critical infrastructure and key resources (CI/KR) of the United States is essential to the Nation's security, public health and safety, economic vitality, and way of life. Attacks on CI/KR **could significantly disrupt the functioning of government** and business alike and produce cascading effects far beyond the targeted sector and physical location of the incident. Direct terrorist attacks and natural, manmade, or technological hazards could produce catastrophic losses in terms of human casualties, property destruction, and economic effects, as well as profound damage to public morale and confidence. Attacks using components of the Nation's CI/KR as weapons of mass destruction could have even more devastating physical and psychological consequences.

The overarching goal of the National Infrastructure Protection Plan (NIPP) is to:

*Build a safer, more secure, and more resilient America by enhancing protection of the Nation's CI/KR to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency.*

The NIPP provides the unifying structure for the integration of existing and future CI/KR protection efforts into a single national program to achieve this goal. The NIPP framework will enable the prioritization of protection initiatives and investments across sectors to ensure that government and **private sector resources** are applied where they offer the most benefit for mitigating risk by lessening vulnerabilities,

The NIPP also discussed implementing “Advisory Councils” shown below. These councils have been used as a method to involve the private sector in matters of national security relating to critical infrastructure.

### 2.2.6 Advisory Councils

Advisory councils provide advice, recommendations, and expertise to the government regarding CI/KR protection policy and activities. These entities also help enhance public-private partnerships and information sharing. They often provide an additional mechanism to engage with a pre-existing group of private sector leaders to obtain feedback on CI/KR protection policy and programs, and to make suggestions to increase the efficiency and effectiveness of specific government programs. Examples of CI/KR protection-related advisory councils and their associated responsibilities include:

- **Critical Infrastructure Partnership Advisory Council (CIPAC):** CIPAC is a partnership between government and private sector CI/KR owners and operators that facilitates effective coordination of Federal CI/KR protection programs. CIPAC engages in a range of CI/KR protection activities such as planning, coordination, NIPP implementation, and operational activities, including incident response, recovery, and reconstitution. **DHS published a Federal Register Notice on March 24, 2006, announcing the establishment of CIPAC as a Federal Advisory Committee Act (FACA)<sup>18</sup>-exempt body pursuant to section 871 of the Homeland Security Act (see chapter 4).**

Remember that highlighted part. Read it twice if you have to. The formation of this [Critical Infrastructure Partnership Advisory Council](#) (CIPAC) as FACA-exempt is crucial and I'll explain why later. One more thing regarding membership of CIPAC:

The specific membership of the CIPAC will consist of: (a) The CI/KR owners and operators that are **members of their respective sector's recognized Sector Coordinating Council (SCC)**, including their representative trade or equivalent organizations ["SCC CIPAC Members"]; and (b) Federal, State, local, and tribal governmental entities comprising the members of the Government Coordinating Council (GCC) for each sector, including their representative trade or equivalent organizations ["GCC CIPAC Members"].

Again, I want to emphasize that "membership of the CIPAC will consist of: the Critical Infrastructure/Key Resource (CI/KR) owners and operators that are members of their respective sector's recognized SCC."

What does any of this have to do with the 2020 election?

## Cybersecurity and Infrastructure Security Agency

[On January 6th, 2017, Secretary of Homeland Security Jeh Johnson \(Obama's SHS\) released a statement designating](#) "Election Infrastructure" as a "critical infrastructure subsector" within the existing critical infrastructure sector titled: "Government Facilities". This allowed Election Infrastructure Security to fall under the umbrella of the DHS.

[On November 16, 2018, President Trump](#) signed into law the [Cybersecurity and Infrastructure Security Agency Act of 2018](#) which established the Cybersecurity and Infrastructure Security Agency (CISA). [According to their own website](#), "The Cybersecurity and Infrastructure Security Agency (CISA) is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future." The CISA website lists all 16 of the critical infrastructure sectors but I want to focus on the [Government Facilities Sector](#) because that is where you can find the [Election Infrastructure Subsector](#). The election infrastructure subsector landing page looks like this:

## GOVERNMENT FACILITIES SECTOR - ELECTION INFRASTRUCTURE SUBSECTOR: CHARTERS AND MEMBERSHIP

Below is the membership list for the Government Facilities Sector - Election Infrastructure Subsector

[Collapse All Sections](#)

### Charters

- [Election Infrastructure Subsector Government Coordinating Council Charter - 2021](#)
- [Election Infrastructure Subsector Sector Coordinating Council Charter - 2020](#)

### Membership

Here is the 2020 Charter [Election Infrastructure Subsector Government Coordinating Council Charter-2-9-2020](#) as shown above. Keep in mind that Sector Coordinating Councils(SCC) are from the private sector and are members of Critical Infrastructure Partnership Advisory Council (CIPAC).



# **Election Infrastructure Subsector Coordinating Council Charter**

## **Version 1.2**

Approved 2/15/2018

Updated 2/1/2019

Updated 2/9/2020

### **SECTION 1 – Official Designation**

This charter has been developed as a dynamic document intended to clarify and inform the organizational structures, function, and operating procedures for the organization to be known as the Election Infrastructure Subsector Coordinating Council, abbreviated as the “EISCC.”

### **SECTION 2 – Mission and Purpose**

The mission of the Council is to advance the physical security, cyber security, and emergency preparedness of the nation's election infrastructure, in accordance with existing U.S. law. This mission will be accomplished through voluntary actions of the infrastructure owners and operators represented in the Council, as set forth in Presidential Policy Directive/PPD-21 and related authorities.

The EISCC will serve as the principal asset owner interface with other private critical infrastructure sectors as well as with the Department of Homeland Security (DHS), the U.S. Election Assistance Commission (EAC), the state, local and tribal governments (SLTTs), and the Election Infrastructure Subsector Government Coordinating Council (GCC).

### **SECTION 3 – Objectives and Scope of Activity**

The key objectives of the EISCC are to:

- Serve as the primary liaison between the election subsector and federal, state, and local agencies, including the Department of Homeland Security (DHS), concerning private election subsector security and emergency preparedness issues;
- Facilitate sharing of information and intelligence about physical and cyber threats, vulnerabilities, incidents, and potential protective measures;
- Coordinate with DHS and the EIS GCC to develop, recommend, and review sector-wide plans, procedures, and effective practices in support of infrastructure protection, including training, education, and implementation;
- Represent the election subsector in discussions with other infrastructure sectors, as well as with the EIS GCC, on matters of threat, security, risk analysis, emergency preparedness and response, and other related matters;
- Identify and communicate priorities, obstacles or impediments to effective critical infrastructure security and resilience protection programs and develop/recommend to appropriate authorities actions to mitigate them;
- Provide a mechanism to ensure that the specialized knowledge and expertise of sector operators, owners, and other pertinent representatives is available as a resource.

The EISCC is not designed to create the terms of any solicitation or contract vehicle, and any appearance of its use or actual use to this end could bar an entity involved therein from competition in the contract.

Essentially, the EISCC is a council **made up of members from the private sector** that advises and assists our government with the “physical security, cyber security, and emergency preparedness of the nations election infrastructure”. They do this through “**voluntary actions of the infrastructure owners and operators REPRESENTED in the council**”.

This means that the members of the EISCC are the actual election infrastructure **owners and operators**, and they handle the physical security along with the cybersecurity through their own “voluntary actions”.

They “coordinate with the DHS to develop, recommend, and review sector-wide plans, procedures, and effective practices in support of infrastructure protection, including training, education, and implementation”. They also “make recommendations to appropriate authorities to mitigate impediments to effective critical infrastructure security”.

Section 5 of the charter is critical. Focus on the first paragraph below. “The EISCC **operates under the critical infrastructure partnership advisory council (CIPAC) framework** established by the Secretary of Homeland Security pursuant to section 871 of the Homeland Security Act of 2002 (6 U.S.C. §451)”

### Section 5 – Governance

The EISCC operates under the Critical Infrastructure Partnership Advisory Council (CIPAC) framework established by the Secretary of Homeland Security pursuant to **section 871 of the Homeland Security Act of 2002 (6 U.S.C. §451)**.

EISCC decisions can be made only when there is a quorum—defined as the majority of the members being virtually or physically present. In the event that the Council cannot reach consensus on an issue, it will represent the range of views to all external audiences.

The EISCC shall operate and support in its efforts the implementation of pertinent Presidential Executive Orders and Directives, National Infrastructure Protection Plans, and Sector and

What exactly is “section 871 of the Homeland Security Act of 2002 (6 U.S.C. §451)” I’m going to break this down the best I can.

#### SEC. 871. ADVISORY COMMITTEES.

(a) IN GENERAL.—The Secretary may establish, appoint members of, and use the services of, advisory committees, as the Secretary may deem necessary. An advisory committee established under this section may be exempted by the Secretary from Public Law 92–463, but the Secretary shall publish notice in the Federal Register announcing the establishment of such a committee and

So the EISCC which we know operates under the CIPAC framework is exempt from Public Law 92-463 (screenshot below) and that law establishes “a system governing the creation and **OPERATION** of advisory committees.”

Public Law 92-463  
AN ACT  
To authorize the establishment of **a system governing the creation and operation of advisory committees in the executive branch of the Federal Government, and for other purposes.**

So just to make sure this is clear:

- **DHS has submitted a notice in the federal registry in 2006 (renewed every two years) that CIPAC is exempt from oversight over its creation and operation of advisory committees**
- **The EISCC is operating under the framework of CIPAC.**
- **Therefore, the EISCC is exempt from oversight over its creation and operation.**



Now Back to Section 871 (just read the highlighted part):

**SEC. 871. ADVISORY COMMITTEES.**

(a) IN GENERAL.—The Secretary may establish, appoint members of, and use the services of, advisory committees, as the Secretary may deem necessary. An advisory committee established under this section may be exempted by the Secretary from Public Law 92-463, but the Secretary shall publish notice in the Federal Register announcing the establishment of such a committee and identifying its purpose and membership. Notwithstanding the preceding sentence, members of an advisory committee that is exempted by the Secretary under the preceding sentence who are special Government employees (as that term is defined in section 202 of title 18, United States Code) shall be eligible for certifications under subsection (b)(3) of section 208 of title 18, United States Code, for official actions taken as a member of such advisory committee.

Here is the section 202 of title 18, USC (most important parts highlighted):

**§ 202. Definitions**

(a) For the purpose of sections 203, 205, 207, 208, and 209 of this title the term “special Government employee” shall mean an officer or employee of the executive or legislative branch of the United States Government, of any independent agency of the United States or of the District of Columbia, who is retained, designated, appointed, or employed to perform, with or without compensation, for not to exceed one hundred and thirty days during any period of three hundred and sixty-five consecutive days, temporary duties either on a full-time or intermittent basis, a part-time United States commissioner, a part-time United States magistrate judge, or, regardless of the number of days of appointment, an independent counsel appointed under chapter 40 of title 28 and any person appointed by that independent counsel under section 594(c) of title 28. Notwithstanding the next preceding sentence, every person serving as a part-time local representative of a Member of Congress in the Member’s home district or State shall be classified as a special Government employee. Notwithstanding section 29(c) and (d)<sup>1</sup> of the Act of August 10, 1956 (70A Stat. 632; 5 U.S.C. 30r(c) and (d)), a Reserve officer of the Armed Forces, or an officer of the National Guard of the United States, unless otherwise an officer or employee of the United States, shall be classified as a special Government employee while on active duty solely for training. A Reserve officer

So because the EISCC operates under the framework of CIPAC and is exempt from Public Law 92-463, they are classified as “Special Government Employees”.

Back to Section 871 (just read the highlighted part):

**SEC. 871. ADVISORY COMMITTEES.**

(a) IN GENERAL.—The Secretary may establish, appoint members of, and use the services of, advisory committees, as the Secretary may deem necessary. An advisory committee established under this section may be exempted by the Secretary from Public Law 92-463, but the Secretary shall publish notice in the Federal Register announcing the establishment of such a committee and identifying its purpose and membership. Notwithstanding the preceding sentence, members of an advisory committee that is exempted by the Secretary under the preceding sentence who are special Government employees (as that term is defined in section 202 of title 18, United States Code) shall be eligible for certifications under subsection (b)(3) of section 208 of title 18, United States Code, for official actions taken as a member of such advisory committee.

Subsection b(3) of section 208 of Title 18, United States code reads as follows:

**§ 208**

**TITLE 18—CRIMES AND**

(3) in the case of a special Government employee serving on an advisory committee within the meaning of the Federal Advisory Committee Act (including an individual being considered for an appointment to such a position), the official responsible for the employee's appointment, after review of the financial disclosure report filed by the individual pursuant to the Ethics in Government Act of 1978, certifies in writing that the need for the individual's services outweighs the potential for a conflict of interest created by the financial interest involved; or

So because the EISCC operates under the framework of CIPAC and is exempt from Public Law 92-463 (exempt from oversight), they are classified as “Special Government Employees” and they have been certified that their “services outweighs the potential for a conflict of interest created by the financial interest involved.”

This means our government knows there is a “potential for a conflict of interest created by the financial interest involved” for members of the EISCC because the “official responsible for the employee's appointment” has to certify it. They know there is a conflict of interest for members of the EISCC yet they allow it to operate without oversight.

Why is this so important? Scroll down and check out the member affiliations of the Election Infrastructure Subsector Coordinating Council's 2020 Charter. Try not to shit your pants.

**1. Member Affiliations**

Members of the EISCC include entities (companies, organizations, or components thereof) whose services, systems, products or technology are used by (or on behalf of) State or Local government in administering the U.S. election process.

Such entities should have demonstrable working relationships with federal, state, or local election officials, which may include verifiable registration/accreditation with the U.S. Election Assistance Commission, and/or relevant contractual relationships with SLTT government election offices. Entities whose primary assets are elections-related may be considered for membership.

Each Member representative shall serve until the end of their tenure with their appointing entity, or until the entity self-reports a change in its representation.

The Members of the EISCC can remove a member on two thirds vote of the full membership.

Organizing Members of the EISCC include:

Associated Press (AP) Elections	PCC Technology Inc.
BPro, Inc.	Pro V&V
Clear Ballot Group	Runbeck Election Services
Crosscheck	SCYTL
Democracy Live	SLI Compliance
Democracy Works	Smartmatic
Demtech Voting Solutions	Tenex Software Solutions
Dominion Voting Systems	Unisyn Voting Solutions
ELECTEC Election Services Inc.	VOTEC
Election Systems & Software	Votem
Electronic Registration Information Center	VR Systems
Everyone Counts	
Hart InterCivic	
MicroVote General Corp.	



# Dominion Voting Systems

## Smartmatic

Dominion Voting Systems and Smartmatic were two of the members of the EISCC which “advises and assists” our government with election security by “coordinating with the DHS to develop, recommend, and review sector-wide plans, procedures, and effective practices in support of infrastructure protection, including training, education, and implementation”. They were also making “recommendations to appropriate authorities to mitigate impediments to effective critical infrastructure security”. Read again the EISCC Mission and Purpose.

The mission of the Council is to advance the physical security, cyber security, and emergency preparedness of the nation's election infrastructure, in accordance with existing U.S. law. This mission will be accomplished through voluntary actions of the infrastructure owners and operators represented in the Council, as set forth in Presidential Policy Directive/PPD-21 and related authorities.

Our Government knew there was a conflict of interest because they had to sign a waiver certifying they knew. Yet, the members of the EISCC who were the very companies used for basically every aspect of the 2020 election (machines, ballot printing, etc.) were also in charge of the “physical security, cyber security, and emergency preparedness of the nation's election infrastructure” and they HAD NO OVERSIGHT.

I'm sure other companies here could be flagged, but Dominion and Smartmatic are my focus because they have been in the spotlight of the 2020 election fraud. If you haven't yet, read this article from the Epoch Times showing [A History of Foreign Ties Behind Voting Machines Used in US](#).

This revelation sheds new light [on this statement from CISA which was released on November 12, 2020](#). Dominion Voting Systems and Smartmatic, the very companies accused of committing fraud in this election, we're part of the election infrastructure joint statement claiming “the November 3rd election was the most secure in American history.”

### JOINT STATEMENT FROM ELECTIONS INFRASTRUCTURE GOVERNMENT COORDINATING COUNCIL & THE ELECTION INFRASTRUCTURE SECTOR COORDINATING EXECUTIVE COMMITTEES

Original release date: November 12, 2020

WASHINGTON – The members of Election Infrastructure Government Coordinating Council (GCC) Executive Committee – Cybersecurity and Infrastructure Security Agency (CISA) Assistant Director Bob Kolasky, U.S. Election Assistance Commission Chair Benjamin Hovland, National Association of Secretaries of State (NASS) President Maggie Toulouse Oliver, National Association of State Election Directors (NASED) President Lori Augino, and Escambia County (Florida) Supervisor of Elections David Stafford – and the [members of the Election Infrastructure Sector Coordinating Council \(SCC\)](#) – Chair Brian Hancock (Unisyn Voting Solutions), Vice Chair Sam Derheimer (Hart InterCivic), Chris Wlaschin (Election Systems & Software), Ericka Haas (Electronic Registration Information Center), and Maria Bianchi (Democracy Works) - released the following statement:

“The November 3rd election was the most secure in American history. Right now, across the country, election officials are reviewing and double checking the entire election process prior to finalizing the result.

“When states have close elections, many will recount ballots. All of the states with close results in the 2020 presidential race have paper records of each vote, allowing the ability to go back and count each ballot if necessary. This is an added benefit for security and resilience. This process allows for the identification and correction of any mistakes or errors. **There is no evidence that any voting system deleted or lost votes, changed votes, or was in any way compromised.**

“Other security measures like pre-election testing, state certification of voting equipment, and the U.S. Election Assistance Commission's (EAC) certification of voting equipment help to build additional confidence in the voting systems used in 2020.

“While we know there are many unfounded claims and opportunities for misinformation about the process of our elections, we can assure you we have the utmost confidence in the security and integrity of our elections, and you should too. When you have questions, turn to elections officials as trusted voices as they administer elections.”

[On November 30th, 2020, the Department of Homeland Security renewed the charter again for two more years](#) and with that renewal came the straw that broke the election fraud's back. If you go back to the main [Election Infrastructure Subsector: Charters and Membership landing page](#) and click on the [link for the 2021 version of the charter which was released in February](#), you'll notice something different.



They changed the name from “Election Infrastructure Subsector Coordinating Council” (EISCC) to “Election Infrastructure Subsector Government Coordinating Council” (EIS GCC). It now reads that “EIS GCC membership is composed of government agencies and organizations representing government officials that own, operate, or administer subsector physical or cyber assets, systems, and processes or have responsibility for supporting security and resilience of those assets, systems, and processes.”

February 2021



## **Election Infrastructure Subsector Government Coordinating Council Charter**

### **Article I – Official Designation**

The official designation of this Council is the “Election Infrastructure Subsector Government Coordinating Council,” hereinafter referred to as the “EIS GCC” or the “Council.”

No mention of Dominion or Smartmatic. No mention of the private sector companies from 2020 at all.

Can you say cover-up? Where is congress asking questions about this?

### **Closing**

Everything about the 2020 election points to fraudulent activity. The Arizona Senate has subpoenaed the routers from the Maricopa County Board of Supervisors but the MCBS has not been cooperating. Why haven't they turned over the routers? The AZ forensic auditors need to see internet traffic on those routers to see if anything nefarious took place and to finalize their audit.

Refer back to [the previously mentioned Epoch Times article](#) and check out this screen shot below from that article:

Staple Street Capital, a private equity firm located in New York, purchased Dominion in 2018, [according to a press release](#).

[The securities firm](#) that arranged the transaction, UBS Securities LLC, is a division of UBS Americas Inc., which ultimately falls under UBS Group AG, a company listed on the SIX Swiss stock exchange.

Three out of four board members of UBS Securities LLC are Chinese, at least one of whom appears to reside in Hong Kong, according to Bloomberg. UBS says it was one of the “first international banks to have a local presence” in China in the 1990s. In 2012, it formed the current company, UBS Securities Co. Ltd., which it says is the “first foreign-invested fully-licensed securities firm in China.”

There is also this article [claiming a Swiss bank majority-owned by communist China paid Dominion parent company \\$400 million](#). Finally, this reporting from Catherine Herridge stating [DNI John Ratcliffe Confirmed There Was Foreign Interference in November Elections: Report \(theepochtimes.com\)](#)

Director of National Intelligence John Ratcliffe confirmed that there was foreign interference in the 2020 election, according to CBS correspondent Catherine Herridge.

“Well DNI Ratcliffe leads the 17 intelligence agencies and he has access to the most highly classified information that is held by the US government. And he told CBS News that there was foreign interference by China, Iran, and Russia in November of this year and he is anticipating a public report on those findings in January,” [Herridge](#) said on Dec. 3.

Let’s put two and two together here.

- **Dominion Voting Systems was part of the United States Government sanctioned advisory council that was responsible for election infrastructure security, the DHS knew they had a conflict of interest yet let them operate without oversight.**
- **Multiple reports of financial ties between the CCP and Dominion.**
- **[As the Epoch Times stated](#) “Dominion’s voting technology is currently used in 28 U.S. states and Puerto Rico, according to the firm’s official [website](#). More than 40 percent of American voters cast their ballots through the Dominion system in general elections, including 65 of Michigan’s 83 counties, all 159 counties in Georgia, and 2.2 million voters in Maricopa, Arizona’s largest county, among others.”**

The logical conclusion I come to is that China was able to bypass security measures that Dominion Voting Systems was responsible for implementing, in order to access Dominion Voting Systems own machines resulting in the fraudulent outcome of this election.

That is clearly an act of War, and our own Department of Homeland Security sanctioned it and then covered it up.

Our only saving grace in all of this is the Space Force. Our Military could access those Maricopa county routers without subpoena. They have all the information they need and they have likely had it since November 3rd when they we’re monitoring it live. Trump didn’t leave the security of our election up to CISA and CISA alone. The military was watching.

If Devolution is not real, the only way to rectify this election will be through states decertifying their electors, something that has never been done and something I firmly believe will not work. The Biden administration completely disregarded the will of the American people by colluding with China to steal our election, they will obviously do anything they have to in order to stay in power. They will not cooperate with the decertification process and will not give up their grasp on power even if every state decertifies.

Devolution has to be real because there is no other way we will ever rid ourselves of the corruption in our government.

THE BEST IS YET TO COME

Patel Patriot (<https://t.me/patelpatriotchat>)

## Tip Jars

Paypal Link: [@PatelPatriot](#)

or

Venmo Link: [@patelpatriot](#)

PS: I don’t have a way to contact you individually but I want to say THANK YOU to those who have contributed to the “Tip Jar”. Means more to me than you know. Thank you so much.