Commonwealth of Virginia Blue Book Charter

May 2024

Table of Contents

PROMULGATION

May 22, 2024

Dear colleagues,

The U.S. security posture is entering a flexion point that is of critical importance. It is becoming increasingly clear that nation-state actors are attempting to destabilize U.S. sanctuary by attacking our cyber networks to a) disrupt community lifelines by attacking our critical infrastructure, b) impact public trust through disinformation, and c) compromise DoD's ability to defend the homeland and project power globally. This is not unlike the nuclear threat of the mid-1900s, which terrified the world and the American people and precipitated a greater response than had yet been required of civil defense. In 1950, the National Security Resources Board created a 162-page document with a solid blue cover that outlined a model civil defense structure amidst an emerging threat. The "Blue Book" became the template for legislation and organization until FEMA was established.

VDEM recently received a FEMA Regional Catastrophic Planning Grant (RCPG) to address emerging nation-state threats against the region, and the Commonwealth has contracted with CNA to facilitate a four-phased planning process to develop a coordinated operational process to secure critical infrastructure (private and military), support state and federal operational priorities, support our residents, and ensure continuity of government while under a coordinated cyberattack on U.S. critical infrastructure. The products and experiences will result in a better understanding of emerging threats, document strategies and plans that can used nation-wide, and begin to exercise them in a newly defined unified coordination framework.

The Blue Book Project is officially promulgated by the approval and signature of this Project Charter, by VDEM as the project sponsor and key participating stakeholders. Signature authorizes the project team to begin execution of the project and working group activities in accordance with the terms, conditions, and objectives outlined herein.

Shawn Talmadge
State Coordinator of Emergency Management

Date

BACKGROUND AND VISION

The persistent and evolving threat of nation-state cyberattacks against our homeland poses a significant risk to the nation's and the Commonwealth of Virginia's (hereinafter referred to as "Commonwealth") information and operational technology infrastructure (IT and OT, respectively). These sophisticated adversaries target critical systems, seeking to disrupt essential services, compromise sensitive data, and undermine public trust. Strengthening the Commonwealth's cybersecurity posture is paramount to safeguarding national security, protecting critical infrastructure, maintaining economic stability, and deterring potential adversaries.

Recognizing the urgency of this challenge, the Virginia Department of Emergency Management (VDEM) has been awarded fiscal year 2023 Regional Catastrophic Grant Program funding to prepare the Commonwealth for a coordinated cyberattack from nation-state actors. The Blue Book Project (or "The Project") will prepare for these threats and bolster the Commonwealth's, and its partner's, capabilities.

In alignment with PPD-21[1] and the VDEM mission, The Blue Book Project will enhance the security and resilience of the Commonwealth's critical infrastructure, stakeholders, and community against cyber threats. The Project is informed by the National Response Framework[2] thus ensuring that all activities will be conducted in a scalable, flexible, and adaptable manner that is consistent with existing incident response organization and doctrine. By fostering collaboration among federal, state, local, tribal, and private sector organizations, as well as public and private owners and operators of critical infrastructure, The Project will better prepare the Commonwealth for responding to a coordinated cyberattack from nation-state actors.

PROJECT OVERVIEW

This project will culminate with a comprehensive Concept of Operations (CONOPS) document that will supplement and inform existing emergency plans, including the Commonwealth's Emergency Operations Plan. The CONOPS will outline the overarching operational concept and strategic vision for effectively managing the consequences of a cyber-attack that impacts the Commonwealth's critical infrastructure.

[1] PPD-21 refers to the Presidential Policy Directive—Critical Infrastructure Resilience and Security, which advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure.

[2] The National Response Framework is FEMA doctrine that serves as an all-hazards framework describing how the National Incident Management System (NIMS) is implemented in the United States.

The CONOPS will serve as a roadmap, guiding stakeholder coordination and response efforts, including government agencies, private sector partners, and emergency response organizations.

In addition, The Project team will also undertake a thorough assessment of the current policy landscape, identifying existing policies, funding requirements, potential sources, and any gaps that need to be addressed. Furthermore, The Project will explore the legal authorities necessary for state support to defense agencies in the event of a cyber-attack, ensuring a clear understanding of roles, responsibilities, and jurisdictional boundaries.

The Blue Book Project will culminate in a series of exercises designed to test the documented procedures and coordination mechanisms against realistic cybersecurity scenarios. These exercises will involve key stakeholders and simulate various cyber-attack scenarios, allowing for the identification of strengths, weaknesses, and areas for improvement in the CONOPS document.

The successful execution of this project will enhance the Commonwealth's preparedness and resilience against nation-state cyber threats, bolstering the ability to detect, respond to, and recover from cyberattacks targeting critical infrastructure. By establishing a clear Concept of Operations, identifying necessary policies and legal authorities, and validating the CONOPS through rigorous testing, this project will contribute significantly to the overall cybersecurity posture of the Commonwealth and the protection of the nation's vital assets.

GOALS AND OBJECTIVES

PROJECT GOALS

The goal of this project is to ensure the Commonwealth is poised to manage the consequences of a sophisticated nation-state cyberattack on critical infrastructure OT. Through this effort the Commonwealth will establish and organize opportunities to support critical infrastructure partners during attacks, ensure residents' basic needs can be met, and ensure the military is able to restore operations and continue its mission to protect the homeland and project forces globally while systems are disrupted.

PROJECT OBJECTIVES

The Blue Book project will work to achieve the following four (4) objectives.

(1) Leverage the expertise of stakeholders from the federal, state, local, and private sector to execute activities that help ensure the Commonwealths resilience in the face of growing threats.

(2) Maintain awareness of the evolving threat environment to inform the state's preparedness and response planning and strategies.

(3) Develop strategies and plans that define the overall coordination framework (operations and management) needed to protect Virginia's critical infrastructure and people, and support the military in restoring mission critical functions, as well as outline processes to respond and recover from unavoidable attacks that damage or destroy systems.

(4) Test and assess the state's resilience to threats by implementing an exercise series.

These objectives align to the four phases of The Blue Book Project.

SITUATION OVERVIEW

In recent years, there has been a significant increase in the frequency, sophistication, and severity of cyberattacks. Adversaries, including nation-states, organized criminal groups, and hacktivists, are exploiting vulnerabilities in networks, systems, and supply chains to compromise critical infrastructure, steal sensitive data, and disrupt operations. Cyberattacks on public and private sector IT systems occur frequently, and often result in intellectual property theft, data breaches, resulting in financial losses, reputational damage, and legal liabilities. Small and medium-sized businesses are particularly vulnerable, as they often lack the resources and expertise to implement robust cybersecurity measures.

Cyberattacks can also have direct and indirect impacts on the public. Personal data breaches can lead to identity theft, financial fraud, and other forms of victimization. Attacks on healthcare systems can compromise patient privacy and safety. Mis-, dis-, and mal- (MDM) information campaigns and social media manipulation can undermine public trust and social cohesion. Meanwhile, cyberattacks on critical infrastructure such as energy, transportation, communications, healthcare, water, and financial services may have cascading effects that extend far beyond the initial target. For example, a successful attack on the power grid could lead to widespread blackouts, disrupting other essential services and causing significant economic losses. Similarly, an attack on a major financial institution could undermine public confidence in the financial system and trigger a broader economic crisis.

RISK ENVIRONMENT

SUMMARY

The risk environment for cyberattacks on operational technology, as well as the threats posed by MDM information from nation-state actors such as Russia, China, Iran, and North Korea, is increasingly complex and challenging. These adversaries employ sophisticated tactics, including Advanced Persistent Threats (APTs), supply chain vulnerabilities, zero-day exploits, and attacks on Industrial Control Systems and Operational Technology (OT). They also leverage social media manipulation, hybrid warfare, and election interference to undermine trust and stability. To mitigate these risks, organizations and governments must implement robust cybersecurity measures, conduct thorough risk assessments, develop incident response plans, foster public-private partnerships, invest in public education, and engage in international cooperation. By adopting a proactive, multi-layered approach to cybersecurity and resilience, the Commonwealth can better protect against the threats posed by nation-state adversaries in the digital domain.

CYBER AND OPERATIONAL TECHNOLOGY

While Information Technology (IT) systems are designed to collect, process, and store data to assist in business decision making and communication, Operational Technology (OT) systems control and monitor physical equipment and processes and are typically used in industrial settings. IT and OT systems have different security requirements and face unique cyberthreats.

The risk environment for OT is characterized by a high impact and increasing frequency of cyberattacks, with legacy systems, limited security controls, and the exploitation of third-party connections being major vulnerabilities. The unclear ownership between OT and IT teams, competing priorities, a shortage of skilled professionals, and operational restrictions further complicate the implementation of effective security measures, making OT environments attractive targets for attackers seeking to cause physical consequences and/or significant financial damages.

MIS-, DIS-, MAL- (MDM) INFORMATION

Mis, dis, and mal (MDM) information campaigns can cause or exacerbate an incident by taking advantage of common challenges during consequence management. Foreign adversaries can leverage misinformation, disinformation, and malinformation to manipulate the information environment.

- **Misinformation** is information that is false, but not created or shared with the intention of causing harm.
- **Disinformation** is information deliberately created to mislead, harm, or manipulate a person, social group, organization, or country.
- **Malinformation** is information based on fact, but used out of context to mislead, harm, or manipulate.

NATION-STATE THREATS

Russia

The Office of the Director of National Intelligence's 2023 Annual Threat Assessment indicated that Russia will remain a top cyber threat as it refines and employs its espionage, influence, and attack capabilities. It also indicated that Russia is particularly focused on improving its ability to target critical infrastructure in the United States and in allied and partner countries, because compromising such infrastructure improves and demonstrates its ability to provide credible threats to the US homeland.

China

During the recent investigation into the Volt Typhoon cyber actors, the U.S. confirmed that the People's Republic of China has gained illicit access to many American critical infrastructure systems across telecommunications, energy, water and wastewater, transportation, and other infrastructure sectors. Chinese hackers are pre-positioning themselves on IT networks to enable lateral movement to OT assets to disrupt functions. They are both opportunistic (i.e., willing to take advantage of known vulnerabilities to conduct indiscriminate cyber campaigns) and willing to systematically target and penetrate key systems. Moreover, China would likely employ propaganda and influence operations to magnify the social disruption caused by a cyber-attack on US critical infrastructure, seeking to undermine the legitimacy of USG institutions by portraying the response as inept.

Iran

Iran's growing expertise and willingness to conduct aggressive cyber operations make it a major threat to the security of U.S. and allied networks and data. Iran's cyber operations tend to follow an opportunistic approach, taking advantage of known vulnerabilities and exploits when able to do so. However, Iran has also been linked to hacking groups that have actively targeted U.S. water and wastewater facilities using an Israeli-made computer system. Iran also supports nonstate actors who maintain hacking groups that have been responsible for cyberattacks within the U.S. and partner and ally nations.

North Korea

North Korea's cyber program is a sophisticated and agile threat actor, with capabilities in espionage, cybercrime, and disruption of critical infrastructure services. Its cyber forces have matured in recent years and are fully capable of achieving temporary, limited disruptions of some critical infrastructure networks in the United States. In addition to the well-known hack on Sony Pictures in 2014, North Korean is thought to be response for more than $1 billion in cyber currency theft over the past few years.

WORKING GROUP ORGANIZING AND IMPLEMENTING EFFORTS

WORKING GROUP OBJECTIVES

A cohesive working group structure will contribute to the Commonwealth's understanding of threats, critical infrastructure vulnerabilities and plans for executing consequence management. Comprised of state, federal, military, and private sector institutions, each working group will identify and document functional group roles and responsibilities to:

1. Conduct a threat assessment;
2. Conduct a critical infrastructure vulnerability assessment to better understand cascading impacts to the public; and
3. Plan for and execute consequence management.

To accomplish these goals, The Project team will lead each working group through a series of scenario-based workshops that include elements of design-thinking and gaming. These workshops will provide structure to working group meetings, helping to work toward clear outcomes and deliverables that comprise input into a single draft CONOPS. The Project team will then validate the CONOPS through a final exercise series, using the outcomes to develop a final CONOPS that represents group consensus.

MEMBERSHIP SELECTION

To meet these objectives, VDEM will organize state, federal, military, and private sector institutions into functional groups. Organization by functional groups (rather than threats, vulnerabilities, and consequences) will decrease the burden on public and private sector stakeholders to find representatives to participate in all working group meetings. VDEM will work with existing contacts in the critical infrastructure and operational technology space to identify working group members.

MEMBERSHIP EXPECTATIONS AND INFORMATION MANAGEMENT

Working group members are expected to participate in each working group meeting and provide feedback on relevant materials, as requested. Working group members may be asked to contribute to or review draft documents that contain sensitive information. Members will not distribute materials or discuss meetings with persons outside of the working group.

Effective information management during this project will enhance productivity, data security, decision-making and compliance. Information management processes will adhere to the following guidelines.

- Information will be classified based on sensitivity (e.g., public, confidential, restricted) and access control will be in place to ensure only authorized personnel can access sensitive data.
- All working group members will be informed of information security best practices.
- Clear guidelines on what can and cannot be shared will be provided.
- Secure communication channels will be used to share information when appropriate.

ROLES AND RESPONSIBILITIES

The roles and responsibilities listed below for project participants align with guidance and direction provided to federal agencies by PPD-21, the VDEM mission, and project guidance.

VIRGINIA DEPARTMENT OF EMERGENCY MANAGEMENT (VDEM)

- Provide overall leadership, direction, and management for The Blue Book Project.
- Define project goals, objectives, and success criteria in alignment with organizational strategies and stakeholder expectations.
- Secure and allocate necessary resources, including budget, personnel, and infrastructure, to support project execution.
- Identify and engage key stakeholders, ensuring their involvement and buy-in throughout the project lifecycle.
- Execute and maintain this project charter, scope statement, and other critical project documents.
- Establish and communicate project governance structure, roles, and responsibilities for all participants.
- Monitor project progress, performance, and compliance with organizational policies and standards.
- Ensure effective communication and coordination among project team members, stakeholders, and external partners.
- Provide regular project status updates and reports to executive sponsors, stakeholders, and governance committees.

ALL WORKING GROUP PARTICIPANTS

- Actively engage in project meetings, discussions, and decision-making processes.
- Provide expertise, insights, and recommendations relevant to their area of responsibility.
- Collaborate with other team members to ensure project success and alignment with organizational goals.
- Communicate openly and transparently, sharing information and updates in a timely manner.
- Adhere to project timelines, deliverables, and quality standards as outlined in the project charter

and plan.

- Maintain confidentiality and protect sensitive information related to the project and the organization.
- Assist in the development and review of project documentation, including requirements, design specifications, and user manuals.

TIMELINE AND MILESTONES

The Blue Book Project will adhere to the following four phase approach over a 2024-2026 project timeframe.

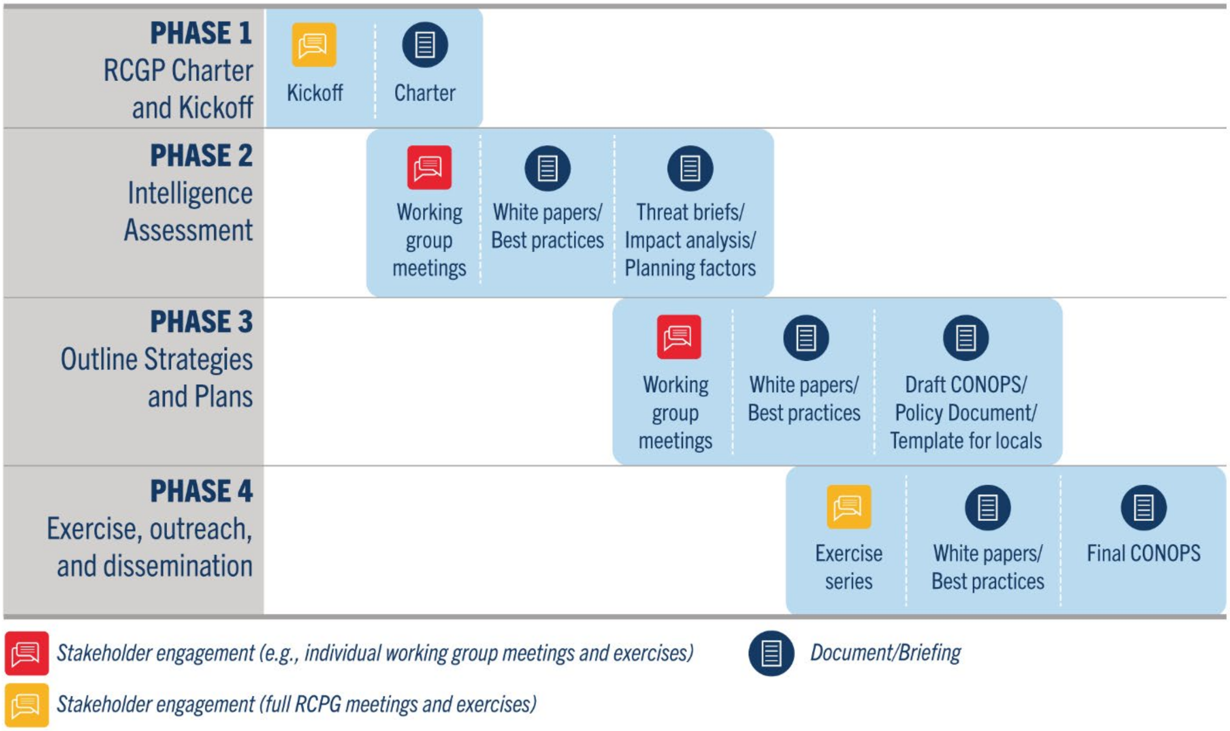

PHASE 1
RCGP Charter and Kickoff
Kickoff
Charter
PHASE 2
Intelligence Assessment
Working group meetings
White papers/ Best practices
Threat briefs/ Impact analysis/ Planning factors
PHASE 3
Outline Strategies and Plans
Working group meetings
White papers/ Best practices
Draft CONOPS/ Policy Document/ Template for locals
PHASE 4
Exercise, outreach, and dissemination
Exercise series
White papers/ Best practices
Final CONOPS
Stakeholder engagement (e.g., individual working group meetings and exercises)
Document/Briefing
Stakeholder engagement (full RCPG meetings and exercises)

Figure 1: Blue Book Project Timeline

The Blue Book Project will include the following deliverables:

Table 1: Blue Book Project Deliverables

Phase 1	**Deliverable 1: Working Group Charter**	A Charter laying out the goals and expectations of the Working Groups, including the project vision, membership and expectations of members, approaches to information sharing, and a timeline.
Phase 2	**Deliverable 2: Intelligence Briefs**	A series of threat-based intelligence analyses on an agreed-upon sources of risk, including specific nation state actors, mis-, dis-, and mal-information, and the cyber threat landscape.
Phase 3	**Deliverable 3: Concept of Operations (CONOPS)**	A comprehensive, CPG 101-conforming CONOPS document that outlines the overarching operational concept and vision for managing the consequences of a cyberattack impacting Virginia's critical infrastructure. The CONOPS will outline how stakeholders will contribute to the four primary missions immediately following an attack, as well as additional critical elements of an actionable CONOPS, including a communications plan, a management plan, and requested external support to enable the response as documented.
	Deliverable 4: Companion Report to CONOPS	Throughout the lifecycle of the project, a running list of recommended policy recommendations; funding requirements, sources, and gaps; and legal authorities needed for state support to defense agencies will be maintained. Towards the end of the project, this aggregated list will be presented to stakeholders and will gather reactions from real time survey questions, polling, and discussion-based techniques to arrive at consensus and form recommendations. The team will then develop the Companion Report to the CONOPS, which outlines these necessary supporting actions, identifies the primary responsible organization, and provides input into how identified gaps may be resolved.
Phase 4	**Deliverable 5: Exercise Series**	A final exercise series to test the CONOPS against realistic cybersecurity scenarios will be conducted at the conclusion of the project.
Ongoing	**Deliverable 6: Whitepapers and Best Practice Guides**	Throughout the lifecycle of the project, targeted white papers and best practice guides on specific topics will be produced.

ADMINISTRATION

MEETINGS

Working groups will participate in a minimum of three (3) meetings in a virtual environment. Prior to meetings, members will receive agendas and any other relevant documentation. Following meetings Working Group members will receive meeting minutes, draft document developed as a result of the meeting, and final documents.

Upon completion of the Working Group stakeholder involvement, project participants will be asked to participate in an in-person exercise series to test the CONOPS.

COMMUNICATIONS

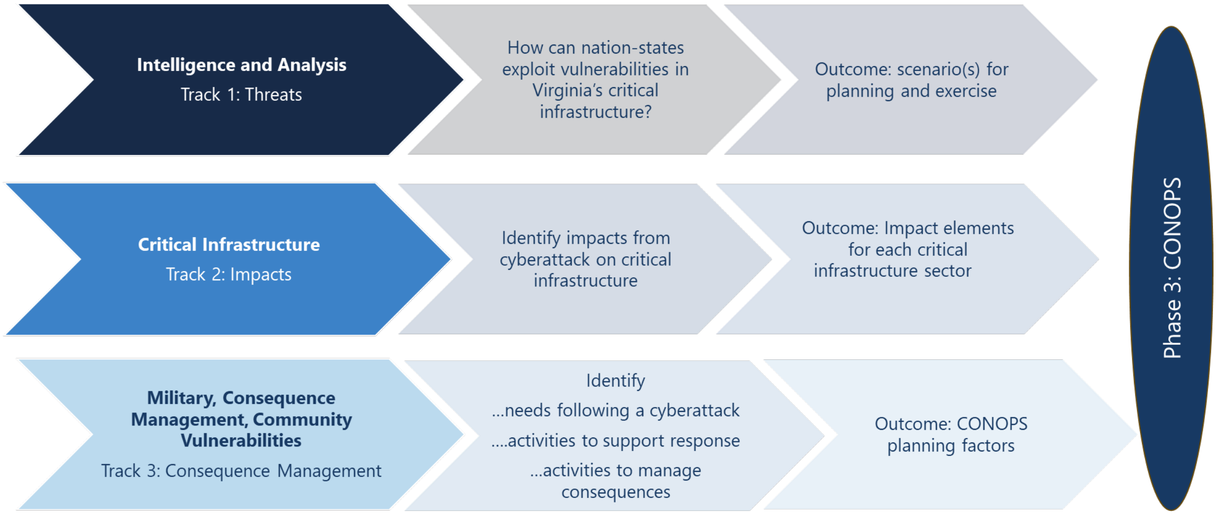
Working Group members will communicate with the project administration primarily through email via the VDEM project email account BlueBook@vdem.virginia.gov.

CHARTER IMPLEMENTATION

This project charter serves as the authoritative document that guides the execution and governance of the Blue Book Project. This charter will be the primary reference for decision-making, problem-solving, and managing stakeholder expectations throughout the project lifecycle.

APPENDIX 1: BLUE BOOK WORKING GROUPS

VDEM has identified five functional working groups to support the execution of this project, each working in parallel along three tracks during phase 2 to identify critical elements and planning factors that will inform the consequence management requirements, roles, responsibilities to be documented in the CONOPS.


Intelligence and Analysis
Track 1: Threats
How can nation-states exploit vulnerabilities in Virginia's critical infrastructure?
Outcome: scenario(s) for planning and exercise
Critical Infrastructure
Track 2: Impacts
Identify impacts from cyberattack on critical infrastructure
Outcome: Impact elements for each critical infrastructure sector
Military, Consequence Management, Community Vulnerabilities
Track 3: Consequence Management
Identify
...needs following a cyberattack
....activities to support response
...activities to manage consequences
Outcome: CONOPS planning factors
Phase 3: CONOPS

.

MILITARY REQUIREMENTS AND SUPPORT WORKING GROUP

The Military Requirements and Support Working Group brings together representatives from various military branches, government agencies, and relevant private sector organizations. The primary objective of this working group is to identify, assess, and address the unique cybersecurity needs and challenges faced by the military.

CONSEQUENCE MANAGEMENT WORKING GROUP

The Consequence Management Working Group brings together representatives from law enforcement agencies, emergency communications, emergency management, government organizations, and relevant private sector entities. The primary objective of this working group is to enhance cybersecurity preparedness and response capabilities in the context of public safety, communications, and emergency management through coordinated consequence management.

INTELLIGENCE AND ANALYSIS WORKING GROUP

The Intelligence and Analysis Working Group brings together experts from intelligence agencies, law enforcement, government organizations, academia, and relevant private sector entities. The primary objective of this working group is to gather, analyze, and share information related to cyber threats, vulnerabilities, and adversaries to support proactive cybersecurity measures and informed decision-making.

CRITICAL INFRASTRUCTURE AND PRIVATE SECTOR WORKING GROUP

The Critical Infrastructure Working Group brings together representatives from government agencies, infrastructure operators, regulatory bodies, and relevant private sector organizations. The primary objective of this working group is to enhance the cybersecurity and resilience of critical infrastructure sectors, such as energy, transportation, water, telecommunications, and healthcare, which are essential to the functioning of society and the economy.

COMMUNITY VULNERABILITIES WORKING GROUP

The Community Vulnerabilities Working Group brings together experts in various potential sources of vulnerability during disasters, such as disabilities and access and functional needs, those requiring both acute and long-term medical care, the very old and very young, and other vulnerable communities. The primary objective of this working group is to address the human needs of a coordinated emergency response to a major cyber incident with real-world, long-term consequences.

GLOSSARY

Advanced Persistent Threat: An adversary with sophisticated levels of expertise and resources that allow the use of multiple different attack vectors, such as cyber, physical and deception, to generate opportunities to achieve objective that establish and extend presence in the information technology infrastructure of organizations. The ultimate goal of these adversaries is to exfiltrate information or undermine the critical aspects of the organization or program's mission.

Critical Infrastructure: The assets, systems, and networks that provide functions necessary for society to function. CISA has defined 16 critical infrastructure sectors: chemical sector; commercial facilities sector; communications sector; critical manufacturing sector; dams sector; defense industrial base sector; emergency services sector; energy sector; financial services sector; food and agriculture sector; government facilities sector; healthcare and public health sector; information technology sector; nuclear reactors; materials, and waste sector; transportation systems sector; and water and wastewater systems.

Concept of Operations: A document that outlines the way that organizations come together to coordinate to reduce risks and vulnerabilities and pre-establish mechanisms for response and recovery.

Industrial Control Systems: Combinations of control components such as electrical, mechanical, hydraulic, pneumatic systems that act together to achieve an industrial objective.

Information Technology: A range of technologies and systems that are used to store, retrieve, process and transmit data for specific uses.

National Response Framework: A FEMA guide that outlines how the United States responds to emergencies and disasters, from small incidents to major catastrophes. The document is based on the National Incident Management System (NIMS), which provides flexible, scalable, and adaptable concepts to align key responsibilities and roles. The document also establishes a comprehensive, national, all-hazards approach to domestic incident response.

Operational Technology: Systems that control and monitor how physical devices perform.

Presidential Policy Directive--21: The Presidential Policy Directive on Critical Infrastructure Security and Resilience that describes the advancement of a national unity of effort to strengthen and maintain secure, function, and resilient critical infrastructure, released on February 12, 2013.