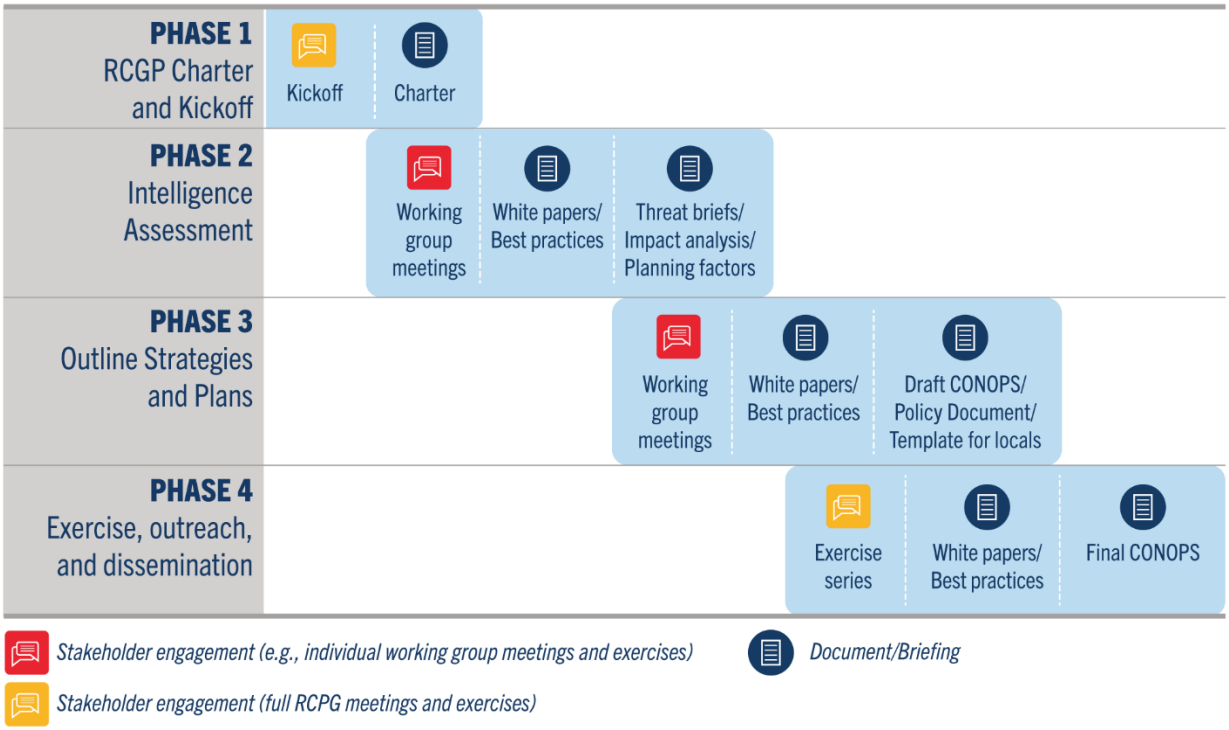
THE BLUE BOOK PROJECT

BACKGROUND

It is becoming increasingly clear that nation-state actors are attempting to destabilize the nation's environment by attacking cyber networks to (a) disrupt community lifelines through attacks on critical infrastructure systems, (b) erode public trust through disinformation, and (c) compromise the ability of the United States to defend the homeland and project power globally. This scenario is not unlike the nuclear threat of the mid-1900s, which terrified the world and the American people and precipitated a greater planning effort 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 amid an emerging threat. The "Blue Book" became the template for legislation and organization until the Federal Emergency Management Agency (FEMA) was established.

To meet the current challenges, the Virginia Department of Emergency Management (VDEM) has undertaken a major consequence management planning effort—the Blue Book Project. The goals of the Blue Book Project are to develop a coordinated operational process to support local, state, federal, and private sector operational priorities; support Virginia residents; and ensure continuity of government while under a coordinated cyberattack on critical infrastructure systems resulting in a national emergency (see the timeline below). This project is funded by a FEMA Regional Catastrophic Preparedness Grant (RCPG), and VDEM has contracted with CNA to develop and support this effort.



The Blue Book Project

CNA

RISK ENVIRONMENT

In recent years, there has been a significant increase in the frequency, sophistication, and severity of cyberattacks. Adversaries, including nation-states, organized criminal groups, hacking groups, private companies, and individuals, are exploiting vulnerabilities in networks, systems, and supply chains to compromise critical infrastructure (such as energy, transportation, communications, health care, water, and financial services), steal sensitive data, and disrupt operations.

Nation-state actors, such as Russia, China, Iran, and North Korea, have been employing increasingly sophisticated tactics. Successful cyberattacks on critical infrastructure will likely result in long-term disruption of services (several weeks or months), have cascading effects that extend far beyond the initial target, and combine information operations to maximize disruptive impact.

When combined with a cyberattack, mis-, dis-, and mal-information (MDM) campaigns can cause or exacerbate an incident by taking advantage of common communications challenges during incident response, undermining public trust and social cohesion, and creating additional challenges for community vulnerabilities, incident response, and consequence management.

PARTNERS

The Blue Book Project is engaging and fostering collaboration among federal, state, local, and private sector organizations, as well as public and private owners and operators of critical infrastructure. Partners will be supporting the Blue Book Project by identifying potential threats and vulnerabilities, exploring likely consequences, and developing response objectives to manage the consequences. Partners will be engaged throughout the 18-month life cycle of the project and will provide expertise, insights, and recommendations relevant to their area of responsibility.

OUTCOMES

This Blue Book Project will result in a comprehensive concept of operations (CONOPS) document that will serve as a strategic framework for public agencies at all levels of government and private sector partners. The CONOPS will guide collaboration and the response efforts necessary to effectively manage the consequences to community lifelines following a cyberattack that disrupts the Commonwealth's critical infrastructure systems for an extended duration. The Blue Book CONOPS will supplement and inform existing emergency plans, including the Commonwealth's Emergency Operations Plan (COVEOP) and a COVEOP Annex for Cyber Response Incidents. However, it is different from existing plans, given the potential for a national emergency resulting from the prolonged outages of critical infrastructure systems and associated consequences to community lifelines while military forces are projecting forces globally in response to the cyberattack. While developing the CONOPS, the Blue Book Project will also produce documentation of the current authorities, regulations, and policies that might inhibit execution and provide this documentation to appropriate levels of government for consideration.

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 cyberattack scenarios to identify strengths, weaknesses, and areas for improvement in the Blue Book CONOPS.

The successful execution of this project will enhance the Commonwealth's preparedness and resilience against nation-state cyber threats, bolstering its ability to detect, respond to, and recover from cyberattacks targeting critical infrastructure. By establishing a clear CONOPS, 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.

For more information, please contact the project planning team at BlueBookProject@vdem.virginia.gov.