2025 NASS IDEAS Award Nomination

Project Title: Government Operations and Key Infrastructure Toolkits (GO-KITs)

Subject Area: Elections; Cybersecurity

Project Description: The Government Operations and Key Infrastructure Toolkit (GO-KIT) is a proactive cybersecurity solution designed for county election offices to swiftly and securely restore critical election operations in the event of a cyber incident. By establishing a logically separated, trusted network, the GO-KIT enables the continuity of essential election functions while safeguarding sensitive data. This innovative solution ensures election systems remain operational and secure, even when the broader county network is compromised.

Submitted by: Washington Secretary of State Steve Hobbs

Contact: Kylee Zabel, Director of Information Security and Response: 360-480-1107, kylee.zabel@sos.wa.gov

Executive Summary

History

The evolving cybersecurity threat landscape presents a formidable challenge to election operations, as adversaries, ranging from cybercriminals to nation-state actors, increasingly target electoral infrastructure to disrupt processes and undermine public trust in democracy. Recognizing that such threats are not a matter of "if" but "when," the Washington Office of the Secretary of State's (OSOS) Information Security and Response Division (ISR) has taken a proactive stance to safeguard the continuity and integrity of election operations.

A defining incident occurred during Washington state's 2023 General Election when a foreign cyber threat actor (CTA) infiltrated a county's information systems through unknown means. This breach escalated into a ransomware attack, disrupting critical election operations in the affected county. Given the federated nature of access to VoteWA—OSOS's statewide election management and voter registration system—a breach in one county posed a potentially substantial risk to the state's entire electoral infrastructure. ISR, in coordination with cross-functional OSOS teams, acted swiftly to secure state systems by revoking the affected county's access to VoteWA until specified security requirements were met. Collaborating closely with the county's IT team, ISR helped develop and execute a response plan that successfully restored essential election operations while the county focused on eradicating the CTA and recovering compromised systems.

While this incident concluded with minimal delay to election processes, it highlighted an opportunity to enhance contingencies, particularly to support counties with limited IT resources, and underscored the potential consequences if multiple counties were targeted simultaneously. The event also occurred during Washington's 18-day voting period—a time when trained election workers are actively processing voter registrations and ballots, verifying signatures, and performing essential duties under close observation by observers—further amplifying the stakes of maintaining operational continuity.

Motivated by its mission to protect Washington's electoral integrity, ISR initiated the development of a reliable, rapid-deployment contingency solution to bolster readiness statewide. This solution, the Government Operations and Key Infrastructure Toolkits (GO-KITs), was designed to ensure that election functions could quickly and securely resume even amid severe cybersecurity incidents. By creating a trusted, logically separated network, the GO-KITs provide secure, limited access to VoteWA and other critical election systems while maintaining the integrity of the broader state infrastructure.

OSOS maintains six fully operational GO-KITs to be deployed to any requesting county elections office experiencing a cyber incident in Washington state. Counties may also furnish their own GO-KITs using funding provided through the Office of the Secretary of State.

By proactively addressing these vulnerabilities and supporting counties in times of crisis, the GO-KITs represent a vital step toward fortifying the resilience of Washington's election infrastructure against evolving cybersecurity threats.

Significance

The GO-KIT project exemplifies best practices in state government by offering an innovative, collaborative, and resource-efficient solution to a critical challenge facing election infrastructure. Its design reflects a proactive, adaptable response to the growing cybersecurity threats targeting elections, ensuring Washington state can maintain the integrity of its election process even in the face of cyber incidents.

Building on lessons learned from a past county cybersecurity breach and tabletop exercises, the ISR established several key criteria for the solution, ensuring it would address the unique needs of local election offices while maintaining flexibility and scalability across diverse county environments.

Targeted Functionality

GO-KITs are specifically tailored to support elections-specific operations by restoring the most essential functions quickly in the event of a cyber incident. Their primary goal is to ensure the continuity of critical election tasks, rather than addressing other business functions that may be affected during an incident. Importantly, the GO-KITs do not resolve or remediate the ongoing cybersecurity incident itself; rather, they provide a secure, temporary solution that allows election operations to continue during disruptive events.

To meet technical requirements, ISR focused on enabling seamless access to VoteWA within 1-2 business days of an incident, even in degraded or contested environments, while ensuring normal operational speeds for critical election functions. Access is restricted to essential systems and services through a carefully managed allowlist, protecting infrastructure from further compromise. To minimize risks, wireless capabilities have been intentionally excluded.

The GO-KITs are designed as a temporary measure to support counties through the election certification process and incident recovery efforts, not as a long-term solution for regular operations. By focusing on the most critical functions, the GO-KITs provide a reliable stopgap to maintain election continuity while addressing long-term recovery needs.

Scalability and Resource Optimization

The GO-KIT solution was specifically designed to address the needs of smaller and medium-sized counties, especially those with limited IT resources. Larger counties, equipped with more robust IT and information security support, often have unique needs based on their internal systems and larger teams. This understanding allowed ISR to scale the GO-KITs effectively to provide tailored support where it was most needed.

To maximize accessibility and sustainability, ISR prioritized a solution that would be both affordable and durable. The resulting GO-KITs feature hardware components with a lifespan of up to 10 years and a total cost of less than $2,000 per kit. Additionally, by leveraging existing county resources—such as unaffected standby laptops, existing networks, and available cables—the cost of the solution can be further reduced, increasing its adaptability to local conditions.

ISR maintains six fully operational GO-KITs, strategically distributed across Washington state to minimize deployment times. With an even distribution between the western and eastern regions, these kits can be quickly deployed to any county experiencing a cybersecurity event. Counties also have the option to assemble their own GO-KITs and be reimbursed through OSOS's

Information Security Funds Program, which provides up to $80,000 per county per state fiscal year for election security enhancements.

The GO-KITs are designed for ease of use, enabling staff with varying levels of technical expertise to deploy them quickly and effectively. This thoughtful, accessible design ensures that all counties, regardless of resources, can maintain election continuity during cybersecurity incidents.

Collaboration and Transparency

The GO-KIT initiative prioritized county involvement at every stage, fostering trust, cooperation, and alignment with the diverse needs of local election offices. Three counties, selected for their varying sizes and IT capabilities, were engaged in virtual briefings and in-person demonstrations of the solution's capabilities. During these trials, county election administrators and IT professionals were encouraged to rigorously evaluate the solution, identify potential weaknesses, and provide actionable feedback. This input proved invaluable in refining the GO-KIT design to ensure its effectiveness across different county environments.

The trial and feedback process yielded significant improvements. For example, ISR was able to reduce the kit deployment time from four hours to just 20 minutes between the first and second demonstrations. These enhancements underscore the importance of collaboration in developing a solution that is both efficient and practical.

Following the trial phase, ISR showcased the GO-KIT at the 2024 Washington Elections Conference, where all counties had the opportunity to learn about the solution. ISR provided a hands-on display of the kit, opportunities to schedule live demonstrations in additional counties, and guidance for counties on purchasing their own kits using available Information Security Funds. This transparent and collaborative approach ensures counties are equipped with additional tools and support to effectively respond to cybersecurity incidents and strengthen election security statewide.

The GO-KIT project directly aligns with the mission of the Office of the Secretary of State to maintain secure, transparent, and efficient elections. By ensuring the continuity of operations during potential cybersecurity disruptions, the GO-KIT strengthens public confidence in the electoral process and exemplifies a forward-thinking approach to risk management in state governance.

Impact/Results

The Go-Kit project has significantly enhanced the resilience of Washington's election infrastructure, delivering substantial benefits to both election operations and citizens.

For county election offices, the GO-KIT provides a secure, reliable solution to restore critical election functions within 1-2 business days of a major cybersecurity incident. This rapid recover minimizes downtime, mitigates reputational damage, and preserves the integrity of the electoral process. Elections are highly scrutinized, and disruptions to key functions such as voter registration and ballot processing can erode public trust. By ensuring these critical operations continue with minimal interruption, the GO-KIT helps maintain voter confidence and safeguard the

integrity of election systems. The project underscores Washington's commitment to secure, transparent elections and strengthens public trust in the democratic process.

The initiative has seen widespread adoption following its successful pilot phase. After three live demonstrations, two of the pilot counties utilized Information Security Funds to procure their own GO-KITs, while the third county expressed intent to do so in an upcoming funding cycle. Interest in the solution surged after its introduction at the 2024 Washington State Elections Conference, with nine additional counties requesting live demonstrations and several others acquiring their own GO-KITs ahead of the 2024 General Election. This growing demand highlights the project's success in addressing critical needs and its increasing recognition across the state.

The GO-KIT initiative also fostered collaboration between state and local governments, promoting stronger cybersecurity awareness and preparedness among election administrators and their teams. By working together, state and local governments have demonstrated how to address shared vulnerabilities and effectively mitigate cybersecurity risks, setting a standard for cooperative problem-solving.

For voters and Washington citizens, the project reinforces the state's commitment to ensuring secure elections, enhancing public confidence in the electoral process. By enabling the continuity of essential election operations, the GO-KIT ensures that election outcomes are delivered on time, even in the face of cyber threats.

Although designed specifically for the restoration of critical election operations, the GO-KIT concept has broader applicability and can serve as a model for other business areas seeking cost-effective, durable solutions to cybersecurity challenges.

Through its focus on resilience, innovation, and collaboration, the GO-KIT project has delivered meaningful improvements to Washington state's election security, enhancing administrators' ability to protect critical functions in an increasingly digital and vulnerable environment.

Supporting Material

2024 NASS Summer Conference Presentation

Washington Assistant Secretary of State Kevin McMahan and Chief Information Security Officer Samuel Anderson presented the GO-KIT project at the 2024 NASS Summer Conference in San Juan, Puerto Rico, July 10, 2024.

See attached NASS Summer 2024 Presentation - Go-Kit.pdf.