NORTH Dakota | Information Technology

Be Legendary.

Cybersecurity

Joint Cyber Security Operations Center (JCSOC)

2021-present

IDEA

What Problem or opportunity does the project address:

The JCSOC project addresses the problem of cyber threats and attacks by establishing a joint state Security Operations Center (SOC) that facilitates direct state-to-state and peer-to-peer sharing of cyber threat intelligence. It aims to enhance cybersecurity capabilities, collaboration, and response across multiple states. By leveraging real-time information sharing, common tools, and standardized processes, the JCSOC improves the collective security posture and enables rapid response to cyber incidents that pose risks to online activities, government operations, critical infrastructure, and citizen services. The project also addresses the opportunity for states to work together, beyond physical boundaries or state lines, to combat cyber threats and protect systems and citizens using sophisticated tools and technologies.

Why does it matter?

The JCSOC project matters for several reasons:

- Enhanced Cybersecurity: The project addresses the ever-increasing threat of cyber attacks, which can have severe consequences for governments, businesses, and individuals. By establishing a joint state SOC and promoting collaboration and information sharing, the project strengthens cybersecurity measures and helps protect critical systems and infrastructure.
- Efficient Incident Response: Cyber threats can evolve rapidly, and effective incident response is crucial to minimizing their impact. The JCSOC project enables faster response times by facilitating real-time sharing of threat intelligence, best practices, and playbooks among member states. This collaborative approach allows for a more coordinated and efficient response to cyber incidents.
- Protection of Citizen Services: As governments increasingly rely on digital platforms to deliver services to citizens, safeguarding those services becomes paramount. The JCSOC project aims to protect citizen services by addressing various security risks, such as identity theft, ransomware attacks, phishing attempts, and denial-of-service attacks. By sharing data and intelligence, member states can proactively identify and mitigate threats, reducing the risk to citizens' personal information and ensuring the continuity of essential services.
- Nationwide Cooperation: The JCSOC project is unique in that it promotes nationwide cooperation among states. This level of collaboration goes beyond individual state boundaries, fostering a collective defense approach to cybersecurity. By working together, sharing resources, and leveraging the expertise of cybersecurity teams across states, the project strengthens the overall security posture of the nation and creates a more resilient cybersecurity ecosystem.

- Learning and Knowledge Exchange: The project facilitates the sharing of best practices, skill sets, and knowledge among security operations center (SOC) analysts from different states. This collaboration helps accelerate learning curves when dealing with new and evolving cyber threats. By leveraging the collective expertise and experience of SOC analysts, the project promotes continuous learning and improvement in cybersecurity practices.

In summary, the JCSOC project matters because it enhances cybersecurity, improves incident response, protects citizen services, fosters nationwide cooperation, and promotes learning and knowledge exchange. By addressing the challenges posed by cyber threats through collaborative efforts, the project contributes to a more secure and resilient digital environment.

What makes it different

The JCSOC project stands out and is different from traditional cybersecurity initiatives in several ways:

- Joint State Collaboration: The project establishes a joint state Security Operations Center (SOC) that enables direct state-to-state and peer-to-peer sharing of cyber threat intelligence. This level of collaboration goes beyond individual state boundaries and encourages states to work together as a collective defense against cyber threats. It promotes a unified and coordinated approach to cybersecurity across multiple states.
- Real-time Information Sharing: The JCSOC project emphasizes real-time sharing of threat intelligence, best practices, and playbooks between member states. This enables rapid response to cyber incidents and facilitates timely and effective decision-making. The ability to exchange information in real-time enhances the overall cybersecurity posture and helps member states stay ahead of evolving threats.
- Common Tools and Processes: The project promotes the use of common tools, systems, and playbooks across member states. It establishes a standardized approach to cybersecurity operations, leveraging a Security Orchestration Automation and Response (SOAR) system, a common taxonomy (Veris), and a Malware Information Sharing Platform (MISP). This consistency in tools and processes facilitates seamless collaboration and enables efficient information exchange between states.
- Multi-State Cybersecurity Teams: The JCSOC project encourages collaboration among SOC analysts from different states. This collaboration allows for the sharing of best practices, knowledge transfer, and the development of collective expertise. It reduces the learning curve when working with new and complex cyber threats and strengthens the overall skill sets of cybersecurity professionals involved.
- Nationwide Scope: The JCSOC project is a nationwide initiative that aims to protect a significant portion of the United States, covering more than 20% of the nation. It demonstrates an unprecedented level of cooperation and collaboration among states, emphasizing the importance of working together to address cyber threats that transcend individual state boundaries.

By combining joint state collaboration, real-time information sharing, common tools and processes, multi-state cybersecurity teams, and a nationwide scope, the JCSOC project sets itself apart as an innovative and comprehensive approach to addressing cyber threats. It promotes a proactive and unified defense against cyber attacks, leveraging the collective strength and expertise of member states to enhance overall cybersecurity resilience.

What makes it universal?

The JCSOC project has universal aspects that apply to all states:

- Cybersecurity Challenges: Cybersecurity threats are universal and affect all states, regardless of their size, location, or resources. The JCSOC project addresses the common challenge of protecting critical systems, infrastructure, and citizen services from cyber threats that have the potential to impact any state.
- Information Sharing Mandates: The project aligns with state and federal mandates that emphasize the importance of information sharing and collaboration in the realm of cybersecurity. By establishing a joint state SOC and facilitating direct state-to-state sharing of cyber threat intelligence, the JCSOC project supports the fulfillment of these mandates.
- State CIO Top Ten Priorities: The JCSOC project directly aligns with the State CIO Top Ten Priorities, particularly in the areas of cybersecurity and information sharing. Cybersecurity is consistently identified as a top priority for state CIOs, and the JCSOC project offers a collaborative approach to addressing this priority by fostering cooperation, sharing best practices, and leveraging collective resources.
- Collective Defense Approach: The concept of collective defense against cyber threats is universal to all states. The JCSOC project promotes a shared responsibility model where states work together as one, transcending individual state boundaries, to protect systems, citizens, and critical infrastructure. This collaborative approach is applicable and beneficial to all states, regardless of their specific cybersecurity challenges.

By addressing universal challenges such as cybersecurity threats, complying with information sharing mandates, aligning with State CIO Top Ten Priorities, and promoting a collective defense approach, the JCSOC project offers a universal framework that can be adopted and adapted by all states to enhance their cybersecurity capabilities.

IMPLEMENTATION

What was the roadmap?

The project was founded in 2021 and has continued to grow, currently protecting more than 20% of the nation. Legal agreements with each state take some time to execute, and we expect to reach 80% of the nation by 2026.

The project is ongoing and evolving, with a gradual expansion planned over several years. The timeline includes the initial establishment of the project in 2021 and a projected target of reaching 80% of the nation by 2026.

Who was involved?

- Legislators: Legislators played a pivotal role in the establishment of the JCSOC project. They advocated for and supported the passage of House Bill 1417 in 2021, which laid the foundation for the project. Their role included providing legislative support, securing funding, and enacting policies to enable the collaboration between states.
- Agency Staff: Agency staff members, particularly those from the state cybersecurity and IT departments, were involved in the implementation and operational aspects of the JCSOC project. They contributed their technical expertise, assisted in the establishment of the joint state SOC, and played a role in sharing best practices and coordinating cybersecurity efforts.
- Vendors: Vendors specializing in cybersecurity technologies, tools, and systems have been engaged in the JCSOC project. Their role included providing necessary software, hardware, and infrastructure support to facilitate information sharing, incident response, and threat intelligence exchange among member states.
- Citizens: While not directly mentioned, citizens can be seen as the ultimate beneficiaries of the JCSOC project. The project aimed to enhance the cybersecurity defenses of participating states, protecting critical systems, infrastructure, and citizen services from cyber threats. The involvement of citizens could be through awareness campaigns, education initiatives, or the provision of secure online services.
- Obtaining buy-in and support from legislators, agency staff, and other stakeholders involved effective communication and engagement strategies. These strategies included sharing the project's objectives, benefits, and potential impact on cybersecurity resilience. A comprehensive communications and marketing plan was developed to raise awareness, gain stakeholder support, and promote adoption of the JCSOC project among the participating states and their respective agencies.

How did you do it?

- Resources: The successful implementation of the JCSOC project required various resources, including financial, human, and time resources. Financial resources were needed for acquiring cybersecurity technologies, engaging vendors, and supporting ongoing operations. Human resources included skilled cybersecurity professionals, project managers, and support staff to oversee and manage the project. Time resources were allocated for planning, development, testing, and ongoing maintenance of the JCSOC infrastructure and operations.
- Technical Architecture: The JCSOC project required a robust and secure technical architecture to facilitate the direct state-to-state sharing of cyber threat intelligence. The architecture focused on ensuring the confidentiality, integrity, and availability of sensitive

information exchanged between member states. It involved leveraging emerging technologies, leading practices, and frameworks in the field of cybersecurity to enhance incident response capabilities, threat intelligence analysis, and collaborative information sharing. Privacy and accessibility considerations have been addressed to protect sensitive data and ensure that the system is accessible to authorized users.

IMPACT

What did the project make better?

- Enhanced Cybersecurity Collaboration: The JCSOC project established a joint state SOC that facilitated direct state-to-state and peer-to-peer sharing of cyber threat intelligence. This collaboration between states in the fight against cyber-attacks is unprecedented and demonstrates a significant improvement in inter-state cooperation. It allowed for rapid exchange of threat information, enabling member states to respond more effectively to cyber threats before they impact their systems and citizens.
- Strengthened Incident Response: The project aimed to improve the collective defense posture of member states by working together to address various security risks, including unemployment fraud, ransomware and phishing attacks, identity theft, and denial of service incidents. By leveraging shared playbooks, methodologies, and standardized tools, the JCSOC enhanced incident response capabilities, reducing response times against organized cyber criminals and minimizing the negative impact on government operations and citizen services.
- Nationwide Protection: The expansion of the JCSOC to protect over 20% of the United States signifies a substantial improvement in cybersecurity coverage. The project aims to reach 80% of the nation by 2026, demonstrating a commitment to extend its benefits to a significant portion of the country. By collaborating beyond state boundaries, the JCSOC aims to protect critical infrastructure, prevent fraud and identity theft, and safeguard online activities of citizens across participating states.
- Business Rationale: The JCSOC project matters because it addresses the growing cybersecurity threats that impact governments' ability to serve their citizens. By fostering collaboration, information sharing, and leveraging advanced cybersecurity technologies and practices, the project aimed to mitigate risks, reduce dwell times of threats, and enhance the overall security posture of member states. The project's results align with the business rationale of ensuring the security, integrity, and availability of critical systems and services that citizens rely upon, ultimately safeguarding the interests and well-being of constituents.

How do you know?

Although specific quantitative metrics or comparisons of the environment before and after the project have not been captured, the JCSOC project's overarching goal was to improve cybersecurity resilience, incident response capabilities, and the protection of citizens'

information and services. The project's benefits can be seen in the strengthened collaboration among states, the reduced response time against cyber threats, and the elevated security posture achieved through collective efforts

What now?

- Long-Term Sustainability: Establishing a dedicated team or entity responsible for managing and operating the joint state SOC, ensuring continuous monitoring of cyber threats, updating playbooks and methodologies, and fostering collaboration among member states. Emphasize the importance of long-term commitment and resources to sustain the project's effectiveness and adaptability to evolving cyber threats.
- Cost-Benefit Analysis: Conduct a thorough cost-benefit analysis to showcase the return on investment (ROI) and cost savings/avoidance achieved through the JCSOC project. Quantify the financial benefits resulting from reduced response times, prevention of fraud and identity theft, minimized disruptions to critical infrastructure, and improved incident management. Highlight the potential cost savings compared to individual state-level cybersecurity efforts and emphasize the efficiency gained through collaboration.
- Strategic Importance: Clearly articulate the strategic importance of the JCSOC project in the context of cybersecurity at the state and national levels. Highlight the project's alignment with state and federal mandates, such as addressing key priorities outlined by State CIOs or cybersecurity frameworks. Emphasize the project's contribution to safeguarding citizen services, protecting critical infrastructure, and enhancing the overall security posture of member states. Showcase the project as a vital component of a comprehensive cybersecurity strategy.
- Testimonials and Success Stories: Gather testimonials from stakeholders, such as government officials, agency staff, or constituents, to underscore the impact and value of the JCSOC project. Include feedback highlighting specific instances where the project successfully thwarted cyber threats, protected critical systems, or improved incident response. These testimonials can provide firsthand accounts of the project's efficacy and its positive outcomes.