2025-2027

WASHINGTON STATE

Enterprise IT Strategic Plan: Security

May 2025

Table of Contents

Opening Letter

We are pleased to present Washington State's Enterprise IT Security Strategy. The result of an inclusive process that engaged technology leaders across the state, this strategy is a commitment to ensuring that every digital interaction with government is secure, every partnership strengthens our defenses, and every workforce investment builds a safer tomorrow.

Cybersecurity is not just a technical challenge—it is the foundation of public trust and service delivery. Protecting sensitive data, maintaining secure systems, and preparing for emerging threats are essential to a resilient Washington that serves residents, businesses, and agencies with confidence.

At its core, this strategy is about protecting public trust, strengthening partnerships, and building a skilled cyber workforce. It is built around three goals: ensuring that government services are secure by embedding data protection and security into every interaction with residents, increasing collaboration and resource-sharing to strengthen cybersecurity across all agencies, and investing in a future-ready workforce that can anticipate and respond to evolving cyber threats. These priorities reflect a shared commitment to safeguarding residents, supporting agencies, and securing Washington's digital future.

Our Goals

Earn Trust Through Secure Digital Services

Increase Partnership and Collaboration for a Safer Washington

Shape Tomorrow with a Skilled and Adaptive Cyber Workforce

Our Pillars

Risk Management
Digital Trust
Integrity
Governance

Opening Letter

This strategy is the result of extensive engagement with over 100 security leaders and partners across the state, shaping a roadmap that strengthens our collective resilience while aligning with Washington's broader enterprise IT priorities. However, a strategy is only as strong as its execution.

To achieve this vision, we must work together, take bold action, and embed security in everything we do. Success depends on the collective commitment of agencies, partners, and individuals who recognize cybersecurity is fundamental to public trust and service delivery.

We invite every agency and partner to actively engage in this strategy, align your security priorities, collaborate with goal teams, and take an active role in strengthening Washington's digital defenses.

Sincerely,

Ralph Johnson

State Chief Information Security Officer

Deanna Brocker

Deputy Director, Strategy & Management

Security Strategy Planning Process Overview

The **Enterprise IT Strategic Plan** laid the groundwork for transforming Washington's technology and digital services. Now, the Enterprise IT Security Strategy moves us from planning to action – ensuring cybersecurity is embedded in every aspect of government operations, protecting residents, and strengthening public trust.

Developing this strategy required a collaborative, agency-led effort to identify the priorities, resources, and governance models necessary to turn cybersecurity goals into action. Over 100 security leaders, state agencies, and external partners played a role in shaping this strategy. Through workshops, advisory sessions, and active feedback, participants identified key cybersecurity challenges and opportunities, leading to a unifying statement, three strategic goals, and four foundational pillars.

Advisory group: Guiding the strategy

A Security Strategy Advisory Group was established to provide strategic guidance and ensure that the plan reflects agency needs and priorities. This group included:

- State agency security and IT leaders responsible for implementing cybersecurity programs.
- Representatives from WaTech to align the strategy with statewide policies and oversight.
- Business and technology leaders from key agencies influencing enterprise IT decision-making.
- Experts in risk management, digital trust, and governance to ensure a strong security foundation.

The Advisory Group played a critical role in refining the framework, ensuring that the final strategy is practical, adaptable, and aligned with Washington's long-term IT vision.

Security Strategy Planning Process Overview

Enterprise Security Strategy Approach by the Numbers

2 workshops facilitated

Over 90 security leaders from **30+** state agencies contributed.

1200+ ideas generated and **140+** strategic themes identified

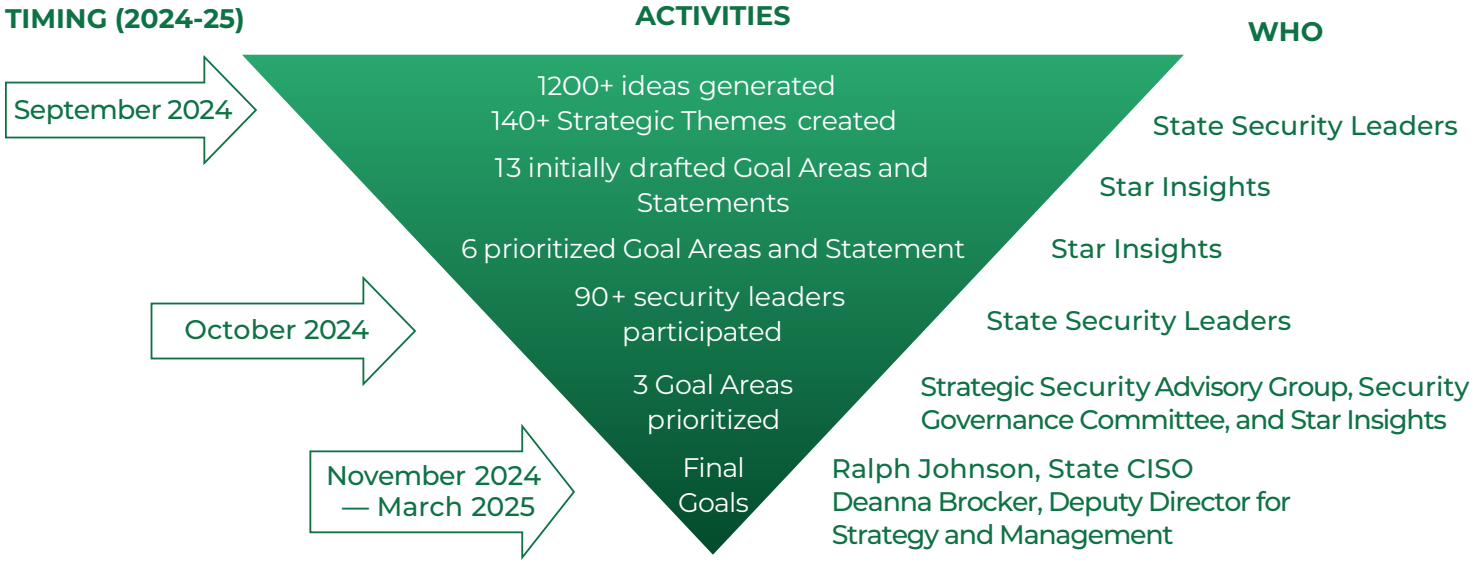
13 initially drafted Goal Areas and Statements drafted

6 prioritized Goal Areas and Statements

1 unifying statement, **3** strategic goals with supporting statements, and **4** foundational pillars

Engagement Model and Planning Timeline

This engagement model leveraged existing governance forums and highly interactive in-person and virtual workshops held across September and October 2024, where more than 100 security and technology leaders across Washington state were invited to participate in brainstorming and planning sessions to shape key priorities for this strategy.



The two in-person workshops saw significant engagement, with agency security, business, and IT leaders sharing their expertise and envisioning bold possibilities for Washington's cybersecurity future. Their input directly shaped the final goals and priorities, ensuring that this strategy is grounded in agency needs and real-world application.

The final refinement stage aligned the prioritized goals and statements with a core set of pillars and a unifying statement, leading to the official launch of Washington's Enterprise IT Security Strategy.

With a strong foundation in place, the focus now shifts to implementation – ensuring that everyone involved plays an active role in building a safer, more resilient Washington.

Moving from Plan to Action

This strategy lays the foundation for a secure, resilient, and digitally trusted Washington, but real success depends on execution. State agencies, local governments, and community partners will play a key role in advancing this work by embedding cybersecurity best practices into daily operations, strengthening partnerships, and investing in a future-ready workforce.

To ensure that this plan translates from strategy to action, implementation will be guided by:

- Goal Teams dedicated to driving progress on cybersecurity priorities, ensuring measurable outcomes across agencies.
- Ongoing governance and oversight through existing IT leadership structures, including engagement with WaTech and interagency governance bodies to align execution with statewide priorities.
- Regular progress reviews that leverage a formal, quarterly business review (QBR) framework and an annual strategic review, ensuring adaptability and responsiveness to emerging challenges.

Cybersecurity is an evolving challenge, requiring agencies to continuously strengthen their security postures. This strategy outlines a pathway to cyber resilience, ensuring agencies can build on existing capabilities, adapt to new threats, and improve response readiness over time. Goal Teams will support agencies in implementing scalable security practices that evolve with changing risks and technology advancements.

Sustained engagement is critical to success. Agencies are encouraged to participate in Goal Teams, align their security initiatives with statewide priorities, and take an active role in strengthening Washington's digital defenses.

For details on how agencies can get involved in implementation efforts, see "**Call to Action: Moving Forward Together.**"

Our Enterprise Security Strategy Framework

Protecting What Matters – Our Residents, Our Systems, Our Future

Goal 1: Earn Trust Through Secure Digital Services

Foster trust and confidence in government services by prioritizing data protection, privacy, and security in every interaction with our residents.

Goal 2: Increase Partnership and Collaboration for a Safer Washington

Enhance cybersecurity and drive innovation through shared responsibility across state agencies and strategic partnerships with local governments, academia, and community partners to ensure all entities (especially resource-limited ones) have the tools to protect their digital environments.

Goal 3: Shape Tomorrow with a Skilled and Adaptive Cyber Workforce

Establish Washington as a national leader in cybersecurity by building a future-ready workforce through recruiting top talent, developing skills in emerging technologies, fostering adaptability, and retaining expertise.

Our Pillars:

Risk Management | Digital Trust | Integrity | Governance

Our Goals

GOAL 1: Earn Trust Through Secure Digital Services

Foster trust and confidence in government services by prioritizing data protection, privacy, and security in every interaction with our residents.

Why this matters:

Trust is the foundation of digital government. Every resident deserves confidence that their personal information is protected and their interactions with state agencies are secure. Cyber threats continue to evolve, making it essential to embed privacy, security, and transparency into every service. Strengthening cybersecurity safeguards will not only protect sensitive data but also enhance the reliability and accessibility of digital government. When security is seamless and proactive, people can engage with government services without hesitation, knowing that their information is safe.

SUPPORTING STRATEGIC PRIORITIES

- Implement a privacy-first service design to ensure security is embedded at every stage of digital service delivery.
- Strengthen cybersecurity policies and data protection frameworks across state agencies.
- Expand security awareness programs and best practices to help agencies and employees protect sensitive data.
- Leverage emerging security technologies to stay ahead of evolving threats.
- Build public confidence through transparent and responsible security practices that reinforce digital trust.

GOAL 2: Increase Partnership and Collaboration for a Safer Washington

Enhance cybersecurity and drive innovation through shared responsibility across state agencies and strategic partnerships with local governments, academia, and community partners to ensure all entities (especially resource-limited ones) have the tools to protect their digital environments.

Why this matters:

A safer Washington is built through shared responsibility and collective action. Cybersecurity threats do not recognize boundaries, and no organization can defend against them alone. Strengthening partnerships between state agencies, local governments, and community partners ensures that all entities, regardless of size, have the tools and expertise to protect themselves. By fostering collaboration, sharing intelligence, and aligning security strategies, Washington will create a stronger, more resilient cybersecurity network that safeguards every community.

SUPPORTING STRATEGIC PRIORITIES

- Expand cybersecurity collaboration across state, local, Tribal, and federal entities to improve information sharing and coordinated response to cyber threats.
- Establish joint security initiatives and partnerships with higher education institutions, nonprofits, and industry leaders to enhance statewide security capabilities.
- Provide security resources and technical assistance to support under-resourced agencies, ensuring equitable access to cybersecurity tools and expertise.
- Create formal security coalitions and working groups that foster knowledge exchange and best practices across agencies.
- Strengthen multi-agency cybersecurity governance structures to align security policies and priorities across the enterprise.

GOAL 3: Shape Tomorrow with a Skilled and Adaptive Cyber Workforce

Establish Washington as a national leader in cybersecurity by building a future-ready workforce through recruiting top talent, developing skills in emerging technologies, fostering adaptability, and retaining expertise.

Why this matters:

The future of cybersecurity depends on people. A workforce that is skilled, adaptable, and ready to lead will define Washington's ability to stay ahead of emerging threats. Investing in training, career pathways, and next-generation skills like artificial intelligence (AI) will ensure that agencies have the expertise to anticipate risks, respond with confidence, and drive security innovation. By cultivating talent and fostering a culture of continuous learning, Washington will set the standard for cybersecurity excellence and prepare for the challenges of tomorrow.

SUPPORTING STRATEGIC PRIORITIES

- Establish cybersecurity training and professional development programs to equip state employees with essential security skills, including AI and emerging technologies.
- Expand career pathways and workforce recruitment efforts to attract top cybersecurity talent through partnerships with higher education, apprenticeships, and internship programs.
- Enhance retention strategies and up-skilling initiatives to ensure cybersecurity professionals remain adaptable to evolving threats.
- Standardize security-related job classifications and competencies across state agencies to streamline hiring, training, and career growth opportunities.
- Create a cybersecurity awareness and innovation culture by integrating security best practices into agency operations and leadership training priorities across the enterprise.

Call to Action: Moving Forward Together

Cybersecurity is a shared responsibility. Every agency, organization, and individual plays a role in protecting Washington's digital infrastructure. This strategy sets the foundation for a more secure, resilient, and trusted digital government, but its success depends on action.

To bring this strategy to life, agencies are encouraged to:

1. Align security priorities with the goals outlined in this strategy to strengthen statewide cybersecurity efforts.
2. Engage with goal teams to contribute expertise, share best practices, and drive meaningful progress.
3. Champion cybersecurity awareness within agencies by embedding security into policies, operations, and workforce development.
4. Collaborate with partners across government, academia, and industry to enhance information sharing and collective security resilience.

This is more than a security strategy – it is a commitment to safeguarding Washington's future. By working together, we can ensure that cybersecurity is not just a technical function but a core value that protects residents, strengthens trust, and enables innovation.

The next step begins now. Join us in making cybersecurity a fundamental part of how Washington serves its people.

Acknowledgments

The Enterprise IT Security Strategy reflects the dedication, expertise, and collaboration of security leaders, agency partners, and technology professionals across Washington. Their collective insights and commitment to strengthening cybersecurity have shaped a strategy that will protect residents, enhance digital trust, and build a more resilient government.

This plan was developed through the contributions of:

- **More than 100+ agency security leaders and partners** who shaped this strategy through their expertise and vision.
- **Enterprise Strategy Advisory Group** provided critical guidance and strategic direction.
- **External advisors and thought leaders/partners** contributed best practices and innovative perspectives.
- **The Enterprise Security Governance committee** lent their leadership in providing valuable benchmarks and guidance.
- **Star Insights Project Team** facilitated an inclusive, strategic planning process.

Thank you to everyone who played a role in developing this strategy. Your efforts will help Washington continue to lead in cybersecurity innovation and resilience.

Contact

For questions or more information regarding this plan, please contact:

Ralph Johnson

State Chief Information Security Officer

ralph.johnson@watech.wa.gov