Washington State

Critical Connections: Protecting the Digital Pulse of Washington's Roads and Rails

PROJECT: Operational Technology – Data Protection/Risk Management

CATEGORY: Cybersecurity Initiatives

PROJECT TIMELINE: June 2023 – Present

Submitted by:

Jesse Regalado
OT Cybersecurity Manager
Washington State Department of Transportation (WSDOT)
Jesse.Regalado@wsdot.wa.gov

EXECUTIVE SUMMARY

As one of the largest and most complex transportation systems in the country, the Washington State Department of Transportation (WSDOT) manages critical infrastructure that millions of residents, businesses, and travelers rely on daily. From the iconic floating bridges of Interstate 90 to the ferry systems and industrial traffic control centers, these environments have increasingly become digital—and increasingly vulnerable.

Recognizing the rising threat of cyberattacks targeting Operational Technology (OT), , the Washington State Department of Transportation (WSDOT), launched a transformative initiative: the **Operational Technology – Data Protection/Risk Management** program. This groundbreaking effort bridges the gap between OT and Information Technology (IT) to establish an integrated, enterprise-level cybersecurity framework. It includes real-time asset discovery, lifecycle governance, continuous monitoring, incident response planning, and the creation of an OT/IT Steering Committee to institutionalize cross-functional collaboration.

By aligning this initiative with NASCIO's top priorities—Cybersecurity, Enterprise Risk Management, IT Governance, Legacy Modernization, and Workforce—WSDOT has pioneered a replicable model for safeguarding digital infrastructure in the public sector. It is not just a technology upgrade—it is a strategic shift toward resilience, continuity, and smarter public service delivery.

PROJECT DESCRIPTION

What problem or opportunity does the project address?

Washington State's extensive and vital transportation infrastructure—including highways, bridges, ferries, rail, and tunnels—is the lifeline of the state's economy and mobility. However, these increasingly digitized systems face growing risks from cyberattacks, aging technologies, and natural disasters. The threat to public safety, commerce, and operational continuity was exacerbated by a lack of visibility and governance over Operational Technology (OT) assets.

WSDOT identified an urgent need to secure its OT landscape, improve collaboration between traditionally siloed OT and Information Technology (IT) teams, and establish a cybersecurity framework capable of protecting critical infrastructure while supporting the agency's modernization efforts.

Why does it matter?

Operational disruptions in OT systems such as traffic signals, bridge control, and ferry operations can have catastrophic implications for public safety and economic activity. The inability to identify, manage, and secure these assets introduces critical vulnerabilities.

Key motivations included:

- Preventing **service outages** and **cyber-induced failures** of bridge and ferry systems.
- Ensuring **compliance with national infrastructure protection goals**.
- Aligning with WSDOT's mission to deliver **safe, reliable, and cost-effective transportation**.

Without intervention, the agency faced:

- Incomplete asset inventories vulnerable to exploitation.
- Limited visibility into device lifecycle risks.
- Delayed threat response capabilities.
- Regulatory and reputational exposure.

What makes it different?

This initiative represents a full paradigm shift from reactive to proactive cybersecurity in the transportation sector. It is distinguished by:

- A **comprehensive convergence of OT and IT** through the formation of the **OT/IT Steering Committee**, which institutionalizes shared governance, risk management, and lifecycle planning.
- The strategic deployment of **OT-specific sensors and tools** in critical environments (e.g., Traffic Management Centers, ferry terminals, industrial control hubs), providing continuous visibility into device health, vulnerabilities, and lifecycle status.
- A **risk-based prioritization model** to allocate resources and address the most critical assets first.
- Integration of vulnerability data into existing systems, streamlining workflows and aligning with **enterprise risk management** goals.

What makes it universal?

As public infrastructure becomes more digitized, every state faces the challenge of safeguarding operational technology (OT) systems. WSDOT's solution addresses a universal problem: legacy OT environments that lack integration with IT governance models, leaving critical systems vulnerable.

This initiative offers a **blueprint for any state agency** responsible for managing complex public infrastructure by:

- Standardizing cybersecurity practices across historically siloed domains.
- Using technology to build resilient, transparent, and scalable operational frameworks.
- Addressing core CIO concerns—security, collaboration, and modernization—within a critical infrastructure context.

This effort directly aligns with several **NASCIO Top Ten Priorities**, including:

- **Cybersecurity and Risk Management**
- **Enterprise Risk Management**

- **Legacy Modernization**
- **IT Governance**
- **Digital Government**
- **Workforce Development**, through upskilling and cross-functional team building.

IMPLEMENTATION

What was the roadmap?

The project followed a strategic, phased roadmap:

1. **Asset Discovery**: Deployed OT-specific tools to map all critical assets across facilities.
2. **Organizational Education**: Conducted training to align security culture with proactive risk posture.
3. **Technology Deployment**: Installed sensors and monitoring tools to feed into centralized systems.
4. **Governance Formation**: Created the **OT/IT Steering Committee** to maintain cross-functional coordination and oversight.
5. **Incident Response Planning**: Tailored response protocols for maritime, industrial, and traffic systems.
6. **Continuous Monitoring**: Enabled real-time data insights for proactive threat and lifecycle management.

Success was defined by the establishment of asset visibility, integration of governance structures, and a scalable operational security model.

Who was involved?

Collaboration was central to success. Key contributors included:

- **WSDOT OT Technicians** – Installed field equipment and mapped operational systems.
- **IT Security Teams** – Integrated monitoring tools and developed threat detection protocols.
- **Engineering & Operations Staff** – Provided operational context and expertise.
- **OT/IT Steering Committee** – Governed long-term strategy and collaboration.
- **Private Sector Partners** – Engaged for surge capacity and incident response preparedness.

WSDOT prioritized stakeholder education, communication, and alignment through workshops, field exercises, and shared documentation.

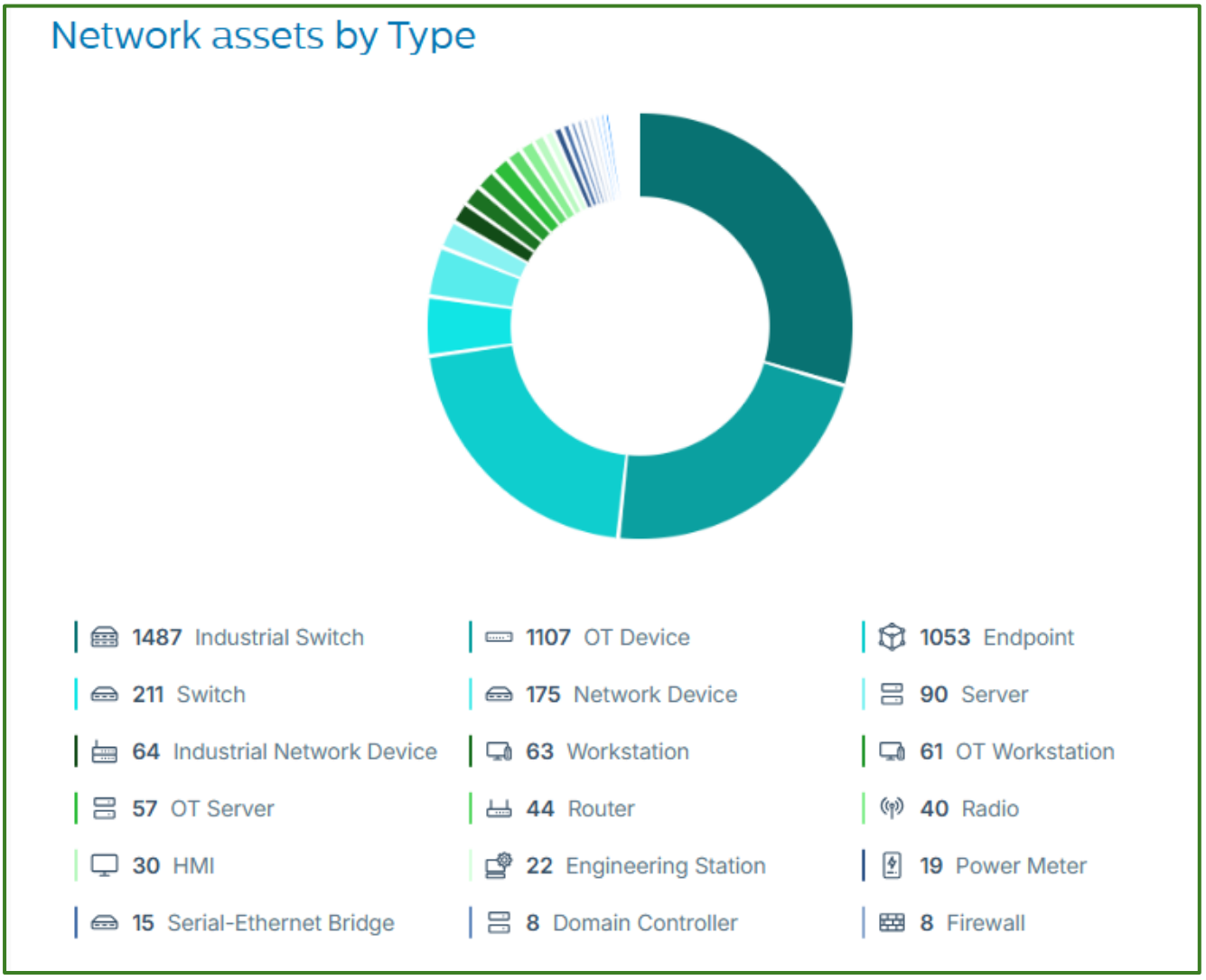
How did you do it?

Resources Required:

- **Financial**: Budget allocated for sensors, software, workforce training, and infrastructure upgrades.
- **Human:** Cross-disciplinary teams from OT, IT, cybersecurity, and operations.
- **Time:** Multi-phase rollout over 12+ months, with iterative learning and expansion.

Technical Architecture:

- OT-specific sensors collect asset and device metadata across transportation facilities.
- Real-time monitoring and risk scoring systems provide proactive alerts and lifecycle insights.
- Integrated vulnerability and asset data feeds support centralized governance and response planning.
- Frameworks conform to the National Information Exchange Model (NIEM) and align with federal infrastructure protection guidelines.



Network assets by type of one network segmentation

IMPACT

What did the project make better?

Before	After
Incomplete visibility into OT assets	Full asset inventory and real-time monitoring
Disconnected OT and IT teams	Unified collaboration through the OT/IT Steering Committee
Reactive incident response	Proactive incident planning and prevention
Isolated systems	Integrated risk management and lifecycle governance
Risk of disruption to bridges/ferries	Strengthened protection of transportation infrastructure

This project transformed WSDOT from a reactive agency to a security-forward organization, resilient against cyber threats to public infrastructure.

How do you know?

Results & Evidence:

- **Institutionalization of governance**: The OT/IT Steering Committee now oversees all cross-domain integration efforts.
- **Technology metrics**: Real-time asset dashboards and lifecycle alerts operationalized in high-risk facilities.
- **Culture shift**: IT and OT teams now engage in joint deployments and shared vulnerability assessments.
- **Incident readiness**: Maritime and transportation-specific response plans are in place and validated.

Testimonial:

> *"This initiative represents more than cybersecurity—it's the future of resilient operations. The OT/IT partnership ensures we're not just reacting to threats but preventing them."*
>
> *— Jesse Regalado, Program Lead, WSDOT*

What now?

The project has transitioned into ongoing operations, governed by the OT/IT Steering Committee and maintained by WSDOT security and engineering teams. Future phases will include:

- **AI-driven threat detection** and **predictive maintenance**.
- Expanded integration with other state and federal transportation security systems.
- Workforce development programs to train future OT/IT specialists.

WSDOT's investment in this initiative has proven transformative, positioning the agency as a national leader in securing public infrastructure. It is a replicable, scalable model that elevates both cybersecurity and public service delivery, making it an ideal candidate for continued support and recognition.

CONCLUSION

The **Operational Technology – Data Protection/Risk Management** initiative has redefined how a state agency secures its most vital infrastructure. WSDOT moved from fragmented awareness to enterprise visibility, from reactive response to proactive protection, and from departmental silos to united governance. This project ensures that Washington's bridges, ferries, tunnels, and traffic systems are not only operational, but resilient, secure, and future-ready.

Its impact extends beyond transportation. By prioritizing cybersecurity at the intersection of operational systems and digital transformation, WSDOT has created a blueprint for other states to follow. The result is a stronger, safer, and more connected public sector, where innovation and infrastructure work together to protect lives and livelihoods.

This is the kind of transformational effort NASCIO was built to recognize—bold, collaborative, and deeply aligned with the mission of modern, secure state IT.