PS2G | PUBLIC SECTOR SOLUTIONS GROUP
Powered by DigiDoc Inc.

OT & IoT Cybersecurity Program

HARTSFIELD-JACKSON ATLANTA INTERNATIONAL AIRPORT

A specialized cybersecurity engagement designed to protect one of the world's most critical transportation hubs from evolving operational technology threats.

PS2G | PUBLIC SECTOR SOLUTIONS GROUP
Powered by DigiDoc Inc.

⚠ CRITICAL CHALLENGE

The Security Gap in Airport Operations

Hartsfield-Jackson Atlanta International Airport relies heavily on Operational Technology (OT) and Internet of Things (IoT) systems that weren't built with modern cybersecurity in mind. These critical systems—from baggage handling and building automation to access control and airfield infrastructure—run on legacy protocols with limited visibility.

This creates significant operational vulnerabilities that put airport safety, regulatory compliance, and public trust at risk. The challenge extends beyond technical debt to fundamental questions of operational continuity.

PS2G Powered by DigiDoc Inc. | PUBLIC SECTOR SOLUTIONS GROUP

Four Critical Vulnerabilities

Operational Vulnerability

Higher risk of cyber incidents that could physically stall or disrupt airport operations, affecting thousands of passengers daily.

Blind Spots

Lack of clear insight into OT/IoT asset health and network behavior across critical systems.

Fragmented Governance

Security standards vary wildly between different vendors and internal teams, creating inconsistent protection.

IT/OT Misalignment

Difficulty integrating specialized operational security into standard enterprise IT frameworks.

PS2G Powered by DigiDoc Inc. | PUBLIC SECTOR SOLUTIONS GROUP

PS2G's Integrated Approach

PS2G integrates OT and IoT cybersecurity into ATL's broader enterprise program while respecting operational constraints. Our methodology is built on four guiding principles that ensure minimal disruption and maximum value.

Risk-Based & Business-Aligned

Security decisions driven by actual business impact and operational priorities.

Non-Disruptive Operations

Assessments and implementations designed to maintain continuous airport operations.

Standards-Driven & Auditable

Full alignment with NIST frameworks for defensible security posture.

Incremental & Scalable

Phased approach that builds capability over time without overwhelming resources.

PS2G | PUBLIC SECTOR SOLUTIONS GROUP
Powered by DigiDoc Inc.

Industry Standards Alignment

NIST SP 800-82 Rev. 3

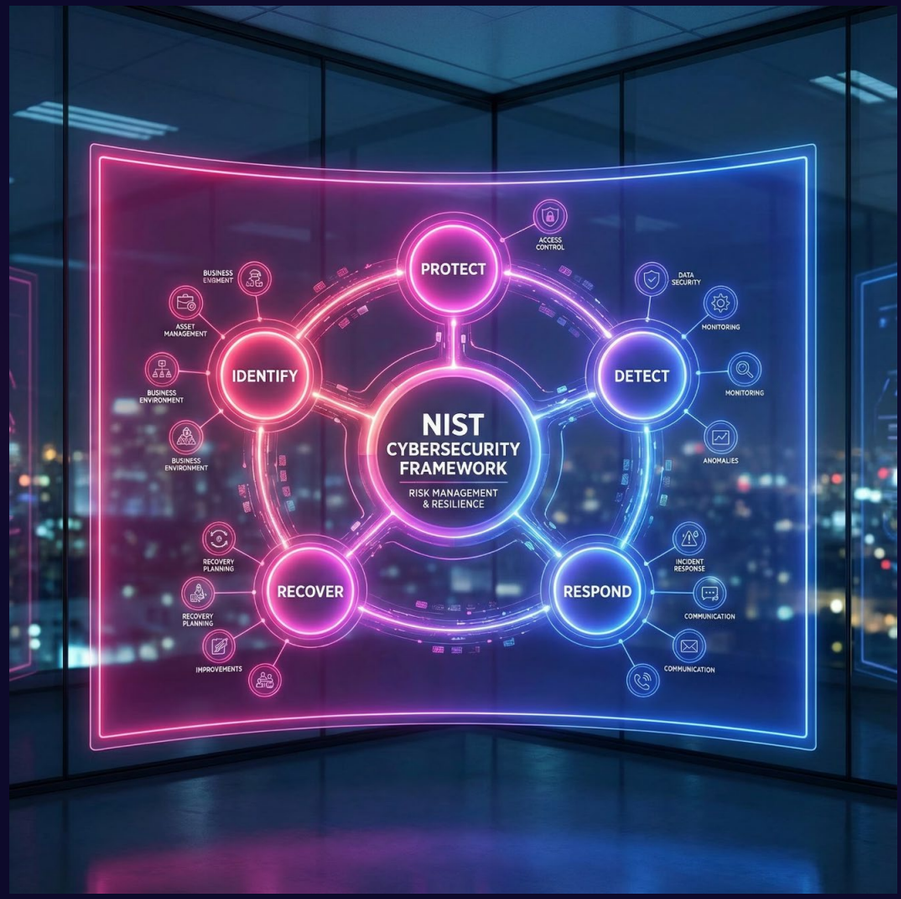
Comprehensive guide to Operational Technology security, specifically designed for industrial control systems.

NIST CSF 2.0

The latest Cybersecurity Framework covering six core functions: Identify, Protect, Detect, Respond, Recover, and Govern.

NIST SP 800-53 Rev. 5

Security and privacy controls for information systems and organizations, ensuring comprehensive coverage.



PS2G | PUBLIC SECTOR SOLUTIONS GROUP
Powered by DigiDoc Inc.

Comprehensive Risk Assessment Methodology

PS2G employs a multi-faceted approach combining three proven assessment methods to ensure thorough evaluation of ATL's cybersecurity posture.

Examination

Evaluates system security mechanisms by examining documentation against established standards and security features.

Interview

Conducts interviews with program management, software development, functional experts, and personnel involved with systems.

Test

Collects and analyzes system security through systematic hands-on and automated measurements of protection mechanisms.

PS2G Powered by DigiDoc Inc. | PUBLIC SECTOR SOLUTIONS GROUP

NIST CSF 2.0: Six Core Functions

Identify

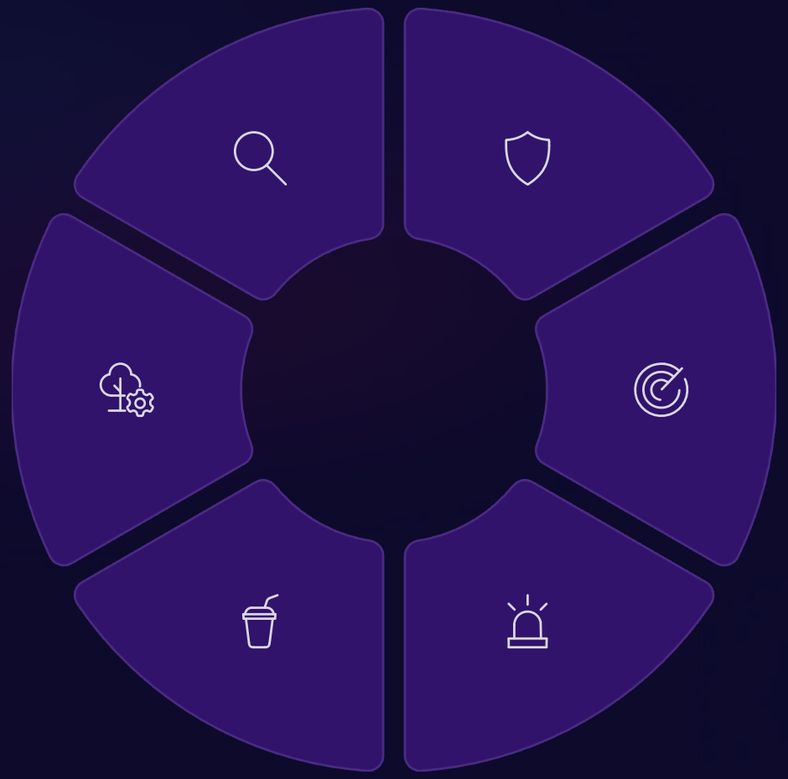
Asset management, business environment, governance, risk assessment, and supply chain risk management.

Govern

Organizational context, risk management strategy, roles and responsibilities, and policy oversight.

Recover

Recovery planning, improvements, and communications to restore capabilities after incidents.



Protect

Access control, awareness training, data security, protective technology, and maintenance procedures.

Detect

Anomalies and events, continuous monitoring, and detection processes across all systems.

Respond

Response planning, communications, analysis, mitigation, and improvements based on incidents.

PS2G Powered by DigiDoc Inc. | PUBLIC SECTOR SOLUTIONS GROUP

PS2G Delivery Team & Tools

PS2G Delivery Team

Cybersecurity Architect

Risk & Compliance Lead

Vulnerability Assessment Lead

Tools

PS2G remains vendor-neutral and will recommend tools based on ATL's existing technology stack and operational requirements, including:

- OT asset discovery and monitoring platforms
- Network segmentation and firewall technologies
- SIEM and SOC integration tools
- Vulnerability and configuration management solutions

PS2G Powered by DigiDoc Inc. | PUBLIC SECTOR SOLUTIONS GROUP

Detailed Project Timeline

A structured 32-day engagement delivering comprehensive risk assessment, analysis, and actionable recommendations.

Days 1-3: Preparation

Initiation, charter, and rules of engagement.

Days 4-6: Context

System categorization and data flow mapping.

Days 7-26: Assessment

Policy review, control assessment, vulnerability scanning, and risk analysis.

Days 27-30: Reporting

Risk assessment report and controls matrix.

Days 31-32: Closing

Executive exit brief and project handover.

PS2G Powered by DigiDoc Inc. | PUBLIC SECTOR SOLUTIONS GROUP

Investment & Cost Structure

PS2G provides transparent, value-driven pricing structured around three core components. Final pricing will be refined based on selected OT/IoT scope and specific systems included in the assessment.

$25K-$40K

Risk Assessment

Comprehensive evaluation of current security posture across all OT/IoT systems.

$15K-$20K

Architecture & Roadmap

Strategic planning and prioritized remediation pathway development.

$50K-$75K

POC / POV

Proof of Concept implementation demonstrating risk reduction and operational value.

Total Investment Range

$90K–$135K

Comprehensive engagement delivering measurable risk reduction and long-term security enhancement for critical airport operations.

PS2G Powered by DigiDoc Inc. | PUBLIC SECTOR SOLUTIONS GROUP

PS2G Qualifications & Experience

PS2G has extensive experience securing operational environments across airports, utilities, and critical infrastructure.

Relevant Experience Includes:

- Nashville International Airport – OT and PCI DSS security testing
- Exelon Corporation – OT cybersecurity policy development
- East Bay Municipal Utility District – OT security assessment
- Multiple NIST 800-53 and NIST CSF implementations

PS2G | PUBLIC SECTOR SOLUTIONS GROUP
Powered by DigiDoc Inc.

Expected Outcomes & Next Steps

Measurable Results

Reduced Operational Risk

Quantifiable decrease in cybersecurity vulnerabilities across critical OT/IoT systems.

Enhanced Visibility

Complete asset inventory and real-time monitoring of OT/IoT infrastructure.

Enterprise Alignment

Seamless integration of OT cybersecurity with existing IT security practices.

Scalable Framework

Replicable model for securing future airport systems and expansions.

Ready to Begin

PS2G recommends initiating Phase 1 with a jointly defined scope to ensure rapid value delivery and minimal operational impact. Upon completion, ATL leadership will have a clear, defensible roadmap for securing OT and IoT systems in 2026 and beyond.

PS2G | PUBLIC SECTOR SOLUTIONS GROUP
Powered by DigiDoc Inc.

Thank You

Thank you for your time and consideration. We look forward to partnering with you.

Contact Information

Address: 7331 Georgia Ave NW | Washington, DC 20012

Phone: 202-299-1011

Email: sales@ps2g.us

Website: www.ps2g.us