IS YOUR AIPORT READY TO MEET THE NEW TSA CYBER AMENDMENTS?

HERE'S HOW HONEYWELL CAN HELP

The Transportation Security Administration (TSA) recently announced new emergency amendments to help enhance security programs with a focus on performance-based measures. Honeywell's in-depth approach to OT cybersecurity can help your airport adapt to the new measures.

TSA REQUIREMENT	**Develop an implementation plan that describes the planned measures designed to improve cybersecurity resilience and prevent disruption and degradation to an airport's infrastructure.**	**Conduct proactive assessments to test the effectiveness of the planned measures.**	**Develop segmented protocols and controls that enable operational technology (OT) systems to continue to operate if IT has been compromised.**	**Create access control policies and prevent unauthorized access to critical cyber systems.**	**Perform continuous monitoring and detection policies and measures to defend against, detect and respond to cybersecurity threats and anomalies that affect critical cyber system operations**	**Minimize system vulnerabilities and potential risks to unpatched networks by applying security patches and updates for operating systems, applications, drivers and firmware or critical cyber systems in a timely manner using risk-based methodology.**
HONEYWELL CYBERSECURITY SOLUTION	Honeywell Cybersecurity Site Assessment (CSA) identifies gaps, provides recommendations and information that supports planning while our Secure Configuration and Design (SCD) enables the design and implementation required by TSA.	Honeywell provides continuous assessment enabled by Vulnerability Assessment and Penetration Testing, as advised by CSA and SCD.	Honeywell follows best practices outlined by CSA, SCD, Incident Readiness and Advisory (IR) to define assigned roles for standard operating procedures to help an airport continue operations in the event of an attack. Honeywell Disaster Recovery (DR) offers back-up, recovery and replication, and a Honeywell Solutions Service Maintenance Contract checks and confirms deployed solutions are providing effective controls and operations.	Honeywell pairs physical security with cybersecurity (portfolio items such as Secure Media Exchange (SMX) USB control, Application Control (AWL), next generation firewall and annual services protect system, node access and solutions integrity) to help address the need for access control measures.	Honeywell Compliance and Risk Monitoring (HCRM) and Advanced Endpoint Security (HAES) provides continuous observation, AI-analysis and response. Honeywell IR helps airports prepare for and respond to threats while Honeywell Threat Defense Platform (HTDP) offers airports breach detection and active defense using deception technology and Honeywell SIEM solution offers airports active monitoring with trend analysis that tracks and alerts anomalous behavior.	Honeywell identifies and minimizes system vulnerabilities with multiple tools. Remote Management (HRM) monitors node performance with patch management; HCRM provides vulnerability risk scoring; and HTDP intrusion detection with active defense through deception.

THE FUTURE IS WHAT WE MAKE IT | Honeywell