

TechBrief

SECURE SERIES III
**ENGINEERED FOR
MISSION-CRITICAL
ENVIRONMENTS.
NOT JUST ADAPTED
FOR IT.**



CHRISTIE®

Federal AV is not commercial AV at scale. The drivers, constraints, and consequences are fundamentally different. In command centers, situation rooms, and intelligence community facilities, display infrastructure is not a productivity tool - it is a mission enabler. Failure is not an inconvenience. It is an operational and strategic liability. Christie Secure Series III was engineered for exactly this reality.

Most commercial LCD displays are adapted for secure environments through software patches and configuration policies. Secure Series III eliminates the attack surface by design. That is not a positioning statement. It is an architectural commitment by design.



TAA COMPLIANT



MULTIVIEW DISPLAY



OPERATIONAL RELIABILITY 24/7



SECURITY FIRST NO WI-FI, NO RF



SCREEN ORIENTATION

Procurement-ready. Compliant by design, not by exception
Federal procurement cycles are long, complex, and unforgiving. Sourcing rejections and compliance gaps do not just delay projects; they kill them. Secure Series III is fully TAA-compliant, with all critical components and manufacturing sourced from TAA-compliant countries. It meets NDAA requirements by eliminating prohibited components and restricted technologies at the source.

This removes procurement risk before it starts. Government approval cycles move faster when compliance documentation is already in hand.

- › Full TAA-compliance documentation available on request
- › NDAA-compliant: no prohibited components, no restricted sourcing
- › Accelerates contract approval and deployment timelines

[Access the TAA and NDAA compliance letter](#)



Security achieved at the foundation.

Not patched in afterwards

In secure AV, every signal path, configuration decision, and firmware update carries security implications. Commercial displays carry Wi-Fi radios, embedded Android or Linux operating systems, and background services that create persistent vulnerabilities. Secure Series III removes these layers entirely.

There is no wireless hardware. No RF capability. No OS-level attack surface. No unauthorized network services. Security is structural - not dependent on software patches that introduce their own risks.

- › Digitally signed and encrypted firmware prevents unauthorized installation and malware injection
- › Tampered firmware cannot execute - blocked at the system level
- › Interface lockdown: LAN, RS-232, IR, and keypad controls can be disabled at the hardware level
- › Supports zero-trust architecture and internal cybersecurity policy enforcement

This is not a commercial platform retrofitted for a secure environment. It is a display system built so that the secure environment does not have to compensate for it.



Purpose-built for secure environments

Volatile memory that classified environments demand, nothing less

Classified environments, SCIF operations, and data recovery risk are not hypothetical concerns. Residual data on display systems is an active vulnerability. Secure Series III automatically erases all displayed content, images, and data the moment the system powers down. No residual data. No extraction risk. No content leakage.

This directly supports secure facility certifications and classified environment compliance requirements.

- › Christie's Statement of Volatility documentation available to support accreditation and audit processes
- › Lifecycle compromise prevented: long-term and mobile deployments stay protected

[Access Christie's Statement of Volatility letter](#)



Mission performance decision superiority starts with what operators can see

Multi-domain operations, real-time situational awareness, geospatial intelligence, and command dashboards demand display performance that eliminates interpretation error. Secure Series III LCD displays deliver native 4K UHD resolution, 500 nits brightness, and 1 billion colors.

Anti-glare treatment and wide viewing angles ensure critical information stays readable across all positions in high-ambient-light command centers and operations rooms. Multi-source viewing capabilities including quad-view, picture-in-picture, and picture-by-picture support complex operational tempo requirements.

- › Built-in input failover: automatic switch to secondary sources if primary input fails

- › Uninterrupted situational awareness during source transitions
- › Engineered for 24/7 continuous operation: industrial-grade components, thermal stability, reliable power systems

Christie is in this market for the long term

Federal systems stay in service for years. They operate in a constantly evolving security landscape. They require sustainment and support processes that commercial refresh cycles do not accommodate. An RMA process designed for a corporate office does not work when a device is installed inside a secure facility.

Christie brings long-term manufacturer commitment to this market - documentation suitable for accreditation and audits, firmware management aligned to security oversight requirements, and warranty and sustainment processes built for secure environments.

- › TAA and NDAA compliance letters available to accelerate government procurement
- › Statement of Volatility documentation available for SCIF and classified facility certification
- › Christie government solutions team supports contract approval, procurement, and deployment timelines



Your next government project starts here

Contact Christie's government solutions team for compliance documentation, technical specifications, and procurement support. We deliver the information required to move your contract approval and deployment forward.

Learn more at:

christiedigital.com/products/lcd-panels/

or contact your Christie representative to discuss your specific facility requirements.



For the most current specification information, please visit christiedigital.com

Copyright 2026 Christie Digital Systems USA, Inc. All rights reserved. Our centers of excellence for manufacturing in Kitchener, Ontario, Canada and in Shenzhen, China are ISO 9001:2015 Quality Management System-certified. All brand names and product names are trademarks, registered trademarks or tradenames of their respective holders. "Christie" is a trademark of Christie Digital Systems USA, Inc., registered in the United States of America and certain other countries. Performance specifications are typical. Due to constant research, specifications are subject to change without notice. CD19005_SECURE_III_datasheet_V3_Feb_26

CHRISTIE[®]