

Axway Solutions for the U.S. Federal Government

Providing security, efficiency and compliance government-wide



Axway has deep expertise in providing the U.S. federal government — including the Department of Defense, the Intelligence Community, federal healthcare organizations and civilian agencies — with scalable, flexible and cost-effective COTS software solutions that have visibility, security and governance capabilities built in.

In a climate that is both politically and economically turbulent, the United States government must become more nimble and capable than ever. Shrinking budgets and smaller teams mean agencies across the board have to find ways to get things done with fewer resources. At the same time, they face more infrastructure modernization and integration requirements, new mandates to move applications to the cloud, and an increase in regulations that bolster cyber security.

Key objectives include:

- Complying with stringent IT-centric regulations including FISMA, HSPD-12, HIPAA and FIPS 201.
- Preventing accidental and malicious security breaches and data spillage.
- Improving user-authentication practices and defending against cyber attacks.
- Quickly and securely moving large volumes of data and large files, even to disconnected or low-bandwidth environments.
- Going paperless to reduce costs.
- Improving communication and service levels within the government and for citizens.

To meet these complex objectives, all areas of the federal government, including defense, intelligence, healthcare and civilian agencies, will need to leverage IT to work smarter — not harder.

Axway solutions enable U.S. government agencies to improve data exchange, consolidate and update systems, secure information and reduce costs — all critical to effectively protecting and serving the American public.



“From now on, our digital infrastructure — the networks and computers we depend on every day — will be treated as they should be: as a strategic national asset.... Given the enormous damage that can be caused by even a single cyber-attack, ad hoc responses will not do. Nor is it sufficient to simply strengthen our defenses after incidents or attacks occur. Just as we do for natural disasters, we have to have plans and resources in place beforehand...”

President Barack Obama,
May 29, 2009¹

Standing guard against cyber threats

In 2009, the White House completed the first Cyberspace Policy Review and made cyber security a top priority for the United States government.

In 2010, there were more than 40 IT security bills before congress addressing:

- Organizational responsibilities
- Compliance and data accountability
- Personal data privacy, data breach handling and identity theft
- Procurement, acquisition and supply-chain integrity

In September 2011, the commander of the new U.S. Cyber Command warned that threats posed by cyber attacks on computer networks and the Internet are escalating from large-scale theft of data and strikes designed to disrupt computer operations to more lethal attacks that destroy entire systems and physical equipment.

So why is federal data and IT infrastructure still vulnerable to cyber threats today? It isn't because of a lack of policies and plans. It is because it's past time to translate policies and plans into an active defense.

Axway provides a flexible and unified commercial off-the-shelf (COTS) platform for creating an active defense against cyber threats. With a secure data exchange and identity security solution in place, agencies throughout the U.S. federal government can shift their focus from reactive measures for post-attack damage control to a proactive strategy for protecting data and infrastructure from current and future threats.

Because Axway's solution does not require “rip and replace” of existing systems or applications, you can quickly establish connections and tightly control access to enable safe, auditable movement of data — whether the information is exchanged by internal or external EDI, ad hoc email or email attachment, web service, or file transfer between applications, systems or individuals.

- **Delivery-based policies** enable you to control who can interact with whom — including government employees, business partners and contractors, and U.S citizens — based on their roles and permissions in your ecosystem.
- **Content-based policies** analyze the content of files and email messages (with attachments as large as 50GB) to automatically identify and secure sensitive data.
- **Digital certificate management, validation, and authorization** protect security-intensive PKI-based transaction networks.

Across Axway products, executive dashboards for compliance officers, technical dashboards for IT, and complete audit trails simplify dispute resolution and lower the cost of compliance with government regulations including DoD 8500.1, HSPD-12 and HIPAA.

¹<http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure>



Axway solutions for the Department of Defense (DoD)

As one of the largest logistical enterprise in the world, the DoD requires the most advanced information exchange and security measures available. Millions of employees exchanging sensitive information, the world's widest public key infrastructure (PKI) deployment, bases and personnel in remote corners of the globe, and a vast and complex supply chain all introduce clear-and-present dangers when it comes to communications and data security, shipping and delivery of supplies, invoicing and payments, and other critical processes.

Axway solutions for the DoD — including all four branches of the U.S. military and virtually every agency and department across the DoD — simplify data exchange, protect information in motion and at rest and prevent unauthorized access to systems and infrastructure with end-to-end security, visibility and control.

Protect email channels with policy-based filtering and encryption

Safeguard your email networks from inbound attacks and outbound data loss with industry-leading encryption, content filtering and policy controls. You can deploy secure email capabilities to any employee or partner with a browser and email client, with support for SSL, S/MIME, PGP and TLS encryption protocols. And, you can analyze, manage, automate and track message delivery all the way to recipients' desktops, no matter where they are located across the globe.

Axway solutions enable the federal government to:

- Centralize and automate control of email security, including protection at the network level and in the DMZ, in alignment with security mandates such as DoD 8500.1.
- Define policies to encrypt and authenticate inbound and outbound email, decrypt and inspect any S/MIME-encrypted email, and validate digital signatures using the Online Certificate Status Protocol (OCSP) – capabilities absolutely critical to the DoD.
- Block spam, viruses and spear-phishing attacks for hundreds of servers using a single management interface.

The Defense Information Systems Agency (DISA) deploys Axway MailGate across the DoD for decryption and inspection of S/MIME-encrypted email – a capability so unique in the industry that MailGate has been adopted as the standard DoD-wide .

Simplify, automate and track file transfer

Exchange critical information internally and externally without the risk of data loss or security breach – even over long distances between disparate platforms and applications, disconnected environments and high-latency connections.

Secure internal and external data exchange

Establish comprehensive and secure connectivity internally and with your civilian

Axway Identity Validation solutions

All four branches of the U.S. military, including virtually every agency across the Department of Defense, rely on Axway for real-time validation of digital certificates within PKI environments.

By ensuring that revoked or invalid credentials cannot be used for secure email, smart card access to physical or logical assets (including wireless), or other sensitive electronic transactions, these security-intensive DoD organizations can ensure the validity and integrity of highly valued and trusted transactions.

For tactical and low-bandwidth environments like Navy ships and the battlefield, the Axway CompactCRL is a satellite-friendly solution that is 50 times smaller than full CRLs.

Axway Identity Validation solutions are CA-neutral and support all widely adopted security standards and open technologies:

- Certified to meet Common Criteria (EAL 3), FIPS 201, NIST PDVAL, FIPS 140-2, and DoD JITC standards
- SCVP compliant (RFC 5055)
- Entrust-ready and IdemTrust-compliant
- Part of the IdemTrust, SWIFT Trust Act, BACS, and Global Trust Authority financial trust infrastructures
- Interoperable with leading cryptographic hardware, including products certified to FIPS 140-2 Level 3 and 4, as well as smart cards such as the DoD Common Access Card and the Federal Personal Identity Verification Card or national eID-card



Intelligence information exchange

Axway's intelligence information exchange solution provides data on demand, moving large volumes of information between domains and across geographies, even to the front line and other remote locations. Exchanging data such as signals, intelligence images and full-motion video is fast and easy, and doesn't require expensive, congested satellite routes.

Information is aggregated, enriched, disseminated and tracked via:

- Automated rules for metadata collection and content enrichment, data mapping/transformation, and web service callouts. Axway uses embedded data to drive dissemination rules and provides a routing structure that can maintain local caches of information in-theater, for sharing across multiple applications.
- Managed and secure file transfer for multiple secure protocols (all PKI-enabled).
- Community management and endpoint provisioning, with easy on-boarding of new data recipients.
- Data exchange visibility, alerting and reporting with real-time tracking and operational dashboards for continuous monitoring.

and military partners, including suppliers, financial institutions and regulatory bodies worldwide. Axway solutions provide wizard-based partner and community management; packaged application integration; out-of-the-box support for EDI, message formats and document handling; and dashboards and alerts for end-to-end visibility.

Axway solutions for the Intelligence Community

The work of the Intelligence Community (IC) is based on the confidential and timely collection, processing, exploitation, dissemination, archiving and retrieval of information. As intelligence gathering platforms have become more sophisticated, they are encountering security, bandwidth and latency problems caused by an explosion in the size and volume of information they need to handle.

Axway solutions address these issues with industry-leading products that protect data in motion and at rest, empowering the IC to exchange information in a timely and efficient manner while maintaining the highest levels of security on high, low, PKI-enabled or public networks. For example, with an Axway solution, you can:

- Quickly transmit large files such as videos to an FOB, without setting up unauthorized FTP sites that violate security protocols.
- Provide up-to-the-minute situational awareness and "information dominance" to front-line commanders, units on the move and forward-deployed analysts.
- Routinely, securely and inexpensively transfer in-theater intelligence to CONUS with no in-field configuration.
- Efficiently handle high-volume, large-file data systems where exploitation and enrichment require sophisticated geospatial analysis or file introspection.
- Authenticate Personal Identity Verification (PIV) cards in real time in compliance with HSPD-12.

Neutralize cross-domain email threats

To guard against both nefarious and accidental data spillage, Axway offers the most widely deployed COTS email guard within the IC. Built to run in classified environments, it is the only solution that can perform policy enforcement for both clear text and encrypted emails and attachments. Other powerful features include IP and email header obfuscation; antivirus, antispam and edge defense; and PKI credential validation.

Solve the "big data" problem with managed, secure ad hoc file exchange

When policy limitations on file size and file types beyond system recognition force employees to "go rogue" with file transfer, the dangerous consequence is that sensitive data can end up traveling over the Internet in the clear, or getting lost altogether.



Rather than turn to dubious workarounds such as personal, unsecured FTP, members of the IC can use Axway's ad hoc file transfer solution to securely send large files (up to 50 GB) from Microsoft Outlook. They simply click a button to attach and send a large file, and automatically and transparently invoke your custom security policies, including content filtering and encryption. Axway also provides secure file transfer services via a zero-footprint web portal that guarantees delivery and data integrity, secures data streaming across the DMZ, supports flexible authentication and repository encryption, and enables effective and efficient auditing.

Both the email and portal options support single sign-on and LDAP integration for easy on-boarding of new users while maintaining the ability to set and enforce global policies beyond your network.

Centralize and track automated file transfer

Axway Managed File Transfer (MFT) solutions enable secure, easy-to-manage information exchange within and outside the IC while adhering to strict government security requirements and reducing the costs and risks associated with file transfer implementation.

Axway solutions for civilian agencies

The highly publicized string of major security breaches in the U.S. over the last few years has led to mounting pressure from the GAO to improve security for government and taxpayer information. At the same time, eGovernment initiatives demand greater transparency and the ability to easily exchange information internally, with citizens (G2C), with businesses (G2B) and with other agencies (G2G).

Axway solutions offer civilian agencies the comprehensive capabilities they need to satisfy both sides of the equation: user authentication, secure file transfer and email security to protect information in motion and at rest, and easy access, complete audit trails, and full visibility into file movement to improve service and ensure that data is appropriately sent and received.

Prevent unauthorized access with Personal Identity Verification (PIV)

Axway Validation Authority (VA) is a fourth-generation, real-time digital certificate validation solution already widely deployed by the DoD and other government agencies. Axway VA makes it easy for civilian agencies to meet HSPD-12 requirements for standardized forms of identification, and adhere to FIPS 201 standards for physical entry into facilities and electronic entry into networks, systems and databases.

Gain control over ad hoc file transfer

As more and more people use email attachments to exchange bigger and bigger files, IT managers have no choice but to impose limits on attachment size. When messages bounce, people find other ways to exchange files — none of which are secure, managed or auditable — feeding a vicious cycle of rising costs and increasing risk.

In addition to implementing cost-cutting and efficiency initiatives, Civilian Agencies must also comply with a growing number of government regulations and mandates, including:

- Federal Information Security Management Act (FISMA)
- Homeland Security Presidential Directive 12 (HSPD-12)
- Federal Information Processing Standards Publication 201 (FIPS 201)
- Health Insurance Portability and Accountability Act (HIPAA)



Combining support for very large file attachments with content-based policy management, encryption, authentication, and tracking capabilities, Axway offers an ad hoc file transfer solution that proactively scans all outbound attachments to prevent data breaches. When a policy violation is detected, countermeasures (including blocking, reporting, or notifying managers) can be applied to protect the information, the agency, and American citizens.

Fully secure email – inbound and outbound, end to end

Axway's secure email solutions prevent data-loss incidents and thwart malicious attacks that can bring down entire email networks. Inbound threat protection includes antispam, virus protection and Intelligent Edge Defense against dark traffic. Outbound protection includes centralized, proactive content filtering, policy enforcement and gateway-to-gateway encryption to protect against accidental data leakage, policy infractions and regulatory violations. Axway also provides a powerful, easy-to-implement email encryption platform that uses robust content filtering capabilities to analyze, manage, protect and report on email traffic.

Establish a secure information exchange platform

Secure data exchange within and outside government walls, especially for bureaus within the Department of the Treasury such as the IRS, requires a comprehensive file transfer strategy that includes data encryption, security policy and governance, and monitoring and testing capabilities. Axway meets all of these requirements to enable secure transfer of all types of files between applications, systems or individuals. In fact, when a recent GAO audit uncovered data exchange vulnerabilities in a large civilian agency, Axway solutions were selected to protect all file transfers between the agency's thousands of internal servers, and between the agency and external entities.

Axway solutions for federal healthcare

Throughout the federal government – and especially in the DoD, Office of the National Coordinator (ONC), Centers for Medicare and Medicaid Services (CMS), Veterans Affairs (VA) and other agencies that involve the healthcare of civilians and military personnel – there is mounting pressure to provide secure, efficient movement of, and accessibility to, health records, claims and benefits information. Elimination of paper processes, adherence to privacy mandates, accurate identity validation and improved patient care are the drivers for change, which promises to be a massive undertaking when you consider things like:

- The VA, healthcare provider and payer to millions of U.S. veterans, processes more than 1.5 million claims each year, and exchanges files of up to 500 pages in length.
- CMS struggles with largely paper-based eligibility and claims processes that make it difficult for seniors and low-income individuals and families to get the care they need – even in emergency situations.



- Within the DoD, soldier health records can be literally scattered all over the world, making it virtually impossible to access and aggregate data in order to provide the best possible care.

Axway solutions drive efficiency, security and collaboration among agencies and healthcare professionals, and simplify compliance with HIPAA, HITECH and other privacy laws.

Achieve secure, paperless managed file transfer

Axway Managed File Transfer (MFT) solutions enable secure communication and data exchange — intra- and inter-agency, and with private health institutions and individuals. Axway simplifies, secures and controls the transmission of images, health records, claims and administrative information; provides end-to-end visibility across applications, systems and platforms; and protects against data leakage with improved governance.

Protect medical records with secure email

As part of an overall data protection strategy, secure email can prevent the leakage of protected health information (PHI), claims data and administrative information. With Axway, sensitive data can be encrypted and email can be digitally signed and scanned for content violations and threats.

Control network access throughout your community

Use Axway's real-time digital certificate validation solution to ensure that only authorized users with valid credentials have access to PKI environments that host patient health records and other sensitive information.

Establish a Health Information Exchange (HIE)

A collaborative HIE can improve healthcare for soldiers in the field, veterans at home, and Medicare and Medicaid patients across the country by making it easy for members of your community to securely exchange data – including lab results, medications and diagnostic images, and claims and administrative data. Axway provides the ideal HIE platform for secure, trackable exchange of clinical information and financial flows, robust partner provisioning and community management capabilities, and the ability to rapidly create and test large numbers of new maps and integration processes — all critically important as you conduct HIPAA 5010 testing in preparation for migration to ICD-10 and HL7.

Your solution, your way

With a flexible architecture and deployment options

Every U.S. government agency has unique IT requirements and capabilities. That's why Axway solutions are based on a flexible "start anywhere, use anything" architecture that lets you select the functionality you need now, while making it easy and straightforward to add new capabilities in the future.

Virtual Lifetime Electronic Record (VLER) project

Currently under development by the U.S. federal government, the VLER is a single electronic system that will track all health and administrative records for military personnel – from the day they enlist throughout the remainder of their lives. VLER is intended to improve the quality of healthcare and services for active duty and veteran service members.



| | |
|---|---|
| Data, process and community integration | |
| Axway B2Bi | Integrate your enterprise with your trading and constituent community, regardless of size or complexity. Axway B2Bi provides a simple way to handle EDI, XML and other applications (such as SAP and Lawson) with a centralized, easy-to-use interface for all configuration, system administration and message management. |
| Managed File Transfer (MFT) — A2A, B2B, ad hoc | |
| Axway Transfer CFT | Gain start-to-finish visibility, policy-based governance and robust community management for secure, auditable and easy-to-manage file exchange within existing infrastructures. |
| Axway SecureTransport™ | A secure, multi-protocol, directory-based Internet file transfer solution that simplifies and secures data transfer across multiple file sites and applications. |
| Axway Interchange | Reliably and securely connect your enterprise with all of your suppliers, partners, distributors, and service providers across private or public marketplaces of any size. |
| Axway File Transfer Direct | Brings enterprise-class managed file transfer (MFT) capabilities to familiar email interfaces and web-based clients and eliminates the problems associated with sending large and confidential files via email. |
| Complete email security | |
| Axway MailGate™ | A robust, easy-to-manage email security solution that provides comprehensive inbound threat protection, outbound data loss prevention and archiving capabilities. |
| Axway Secure Messenger™ | A comprehensive platform that inspects all email at the network gateway, identifies email content that is in violation of enterprise-defined security policies, and automatically redirects suspect messages to a secure, encrypted email channel for further action, such as deletion, quarantine, encrypted delivery, or end-user notification of policy violation. |
| Community management | |
| Axway Endpoints & Provisioning Services | Establish secure last-mile connections with your partners, suppliers and customers over the Internet — quickly, efficiently and reliably. |
| End-to-end visibility and transactional intelligence | |
| Axway Sentinel | Use intuitive business and technical dashboards to monitor MFT/B2B events and Key Performance Indicators (KPIs) in real time. |

For More Information, visit www.axwayfederal.com

Copyright © Axway 2012. All rights reserved.

