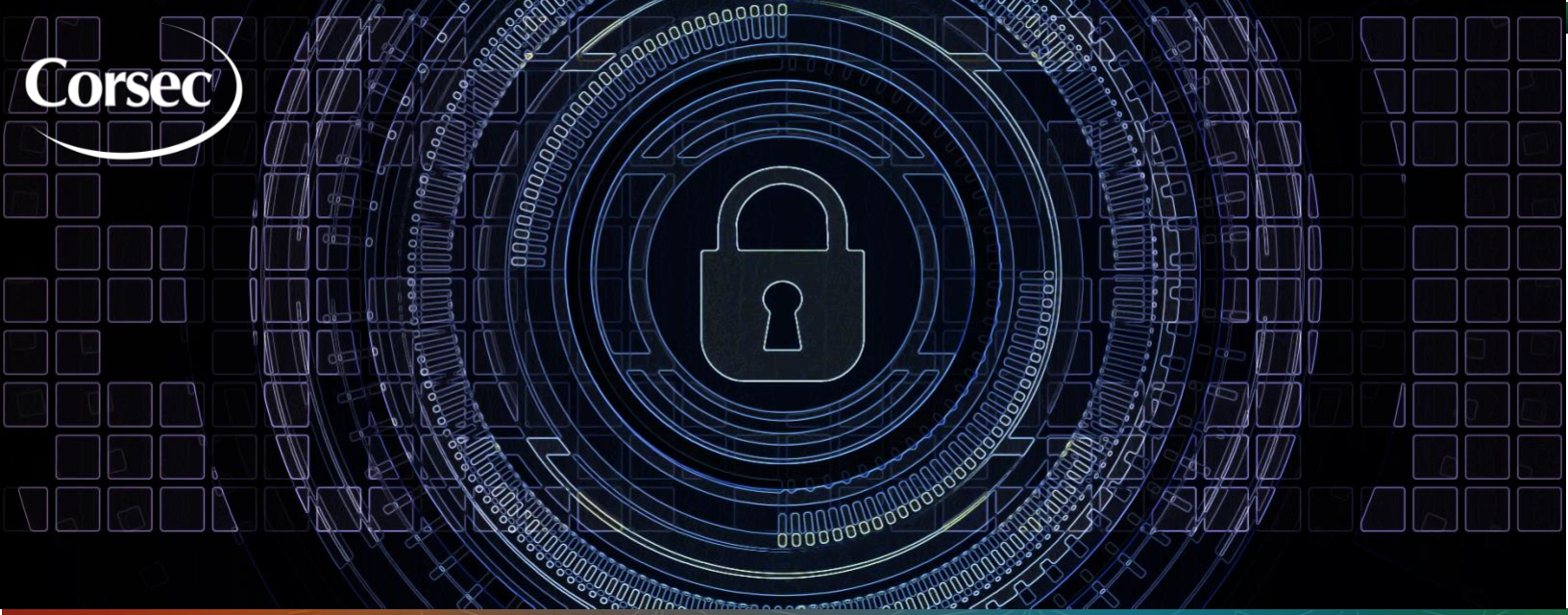


How Information Technology is Changing Government In the 21st Century

Advancements in technology are changing the way federal agencies engage with one another as well as the organizations and citizens that rely on them. With this transition comes a new-found dependence on network communication and security, enabling agencies to send, retrieve, store, and manage the data necessary for domestic and foreign affairs. Though new technology has made this more efficient, it also presents new threats and security vulnerabilities, the likes of which can compromise civilian and government data and open the door to cyberwarfare.

For those tasked with selecting and implementing the policies, procedures, and products designed to secure government and civilian systems, this adds an additional layer of complexity. To navigate this increasingly intricate environment, all stakeholders must have a firm grasp of how the federal landscape is changing, including:

- ✓ Emerging Threats & Technology Trends
- ✓ Government Reaction & Impact
- ✓ Smart Procurement & Mitigating Risk

To understand how to properly safeguard against these attacks, we must first understand the battlegroup; adapting to a new era of cyberwarfare.

A CHANGING FEDERAL LANDSCAPE:
EMERGING THREATS & TECHNOLOGY TRENDS

In 2017, data breaches increased at a drastic rate, over 44% from the previous year, and the outlook for 2018 seems to be no different. Malicious attacks, hackers, global syndicates, and cyber criminals have attempted to infiltrate, commandeer, or otherwise damage valuable national assets and the critical infrastructure for decades. These threats evolve over time, leaving many agencies, including those charged with upholding national security, vulnerable, resulting in wide-reaching damage, the impact of which could be irreparable.

Security breaches have steadily risen over the past 4 years (Figure 1) and according to the Identify Theft Resource Center (ITRC), over 22 million records have been exposed through security breaches since January 1, 2018. These breaches span all industries and categories, including Government/Military, Banking/Credit/Financials, Business, Education, and Medical/Healthcare.

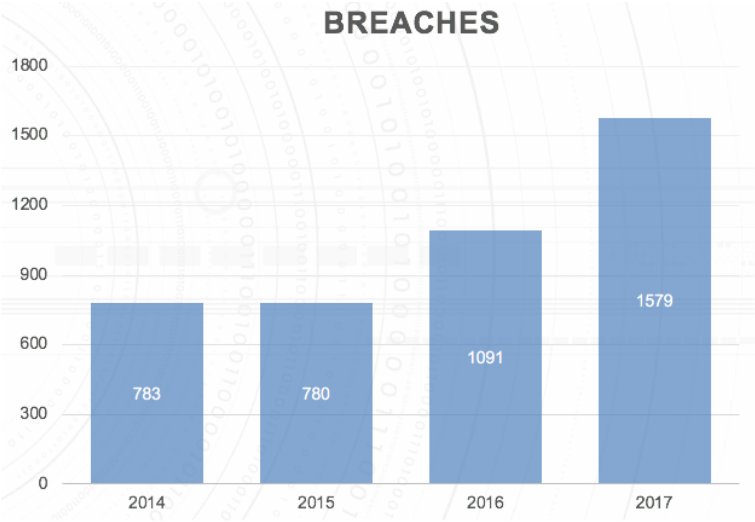


Figure 1 – An incident in which an individual's name plus a SSN, DLN, Medical Record, or Financial Record is put at risk

Over 22 million records have been exposed since January 1st, 2018.

Last year data breaches increased at a rate of over 44% from the previous year.

These security threats are increasing in sophistication, frequency, and overall impact; representing a constant concern for both the private and public sectors as they race to adopt new defense strategies and solutions. The concern is even more significant for the government, as potential breaches can lead to counterintelligence and national security vulnerabilities. Legacy solutions also pose significant risk as weaknesses are overlooked and outdated products continue to be used, leaving systems vulnerable to attacks that have already been addressed in previous patches and new releases.

To mitigate these risks, prevent new attacks, and preserve mission critical resources, security offices have begun to take precautions by establishing defense policies and deploying products and software solutions to defend sensitive data and systems. Unfortunately, defending against attacks that are constantly evolving and learning to penetrate new security products can be daunting and overburdensome. Furthermore, when these protocols fail, the brunt of the breach, specifically the financial impact, can be devastating. Take for example some of the largest breaches and associated financial strain from the past three years:

- U.S. Office of Personnel Management (2015) - Breach that affected 21.5 million users, estimated to cause over $1 Billion in damages
- U.S. Voter Database (2015) - Breach that affected 191 million voters, with damages yet to be known
- Equifax (2017) – Breach that affected 143 million accounts, estimated $439 million in damages

According to a report by the Ponemon Institute, the global cost of data breaches in 2017 averaged $3.62 million, this number was calculated by amassing the unexpected and unplanned loss of customers, the size of the breach/lost records, time taken to identify and contain the breach, detection and escalation measures, and post data breach costs. Although the average cost of a data breach has recently declined (Figure 2), breaches are occurring more frequently and on a larger scale compared to previous years, leaving many concerned over the future of network security and the safety of our nation's critical infrastructure.

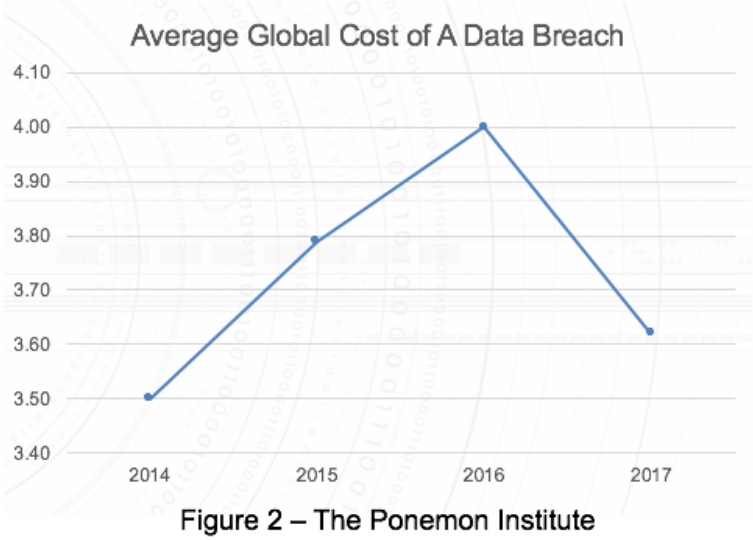


Figure 2 – The Ponemon Institute

Although the average cost of a data breach has declined, companies are experiencing larger breaches than ever.

Why are these threats becoming more frequent? Recent industry trends accompanied by evolving technology solutions play a significant role in this increasingly dangerous landscape. The advancement of cloud technology, the explosion of IoT enabled devices, and development of agile methodologies represent some of the most noteworthy changes within network security, creating an environment where vulnerabilities must be addressed as quickly as they are uncovered.

Cloud services have grown exponentially in both the public and private sectors. Government agencies are spending roughly 22% of their Information Technology (IT) budgets on cloud systems and the expected growth rate averages 17.1% per year through 2021. Cost savings and efficient service delivery have created a shift to cloud-based infrastructures (SaaS, PaaS, and IaaS). Though the cloud offers users insurmountable benefits and potential, it is not without risk.

Prior to cloud implementation, IT departments were able to exercise rigid control over their resources, but public cloud services have decreased that control. As a result, many IT personnel are left with limited visibility over how users interact with critical data on both enterprise- and user-owned devices. This lack of visibility in a sprawling cloud environment also presents security concerns, reducing and sometimes eliminating data management control from the hands of the provider.

This rise in cloud-based architectures and solutions has created a new market for monitoring and visibility sustainment products, alleviating the pain, dangers, and risks that CIOs, security professionals, and network security administrators face.

Internet of Things (IoT) and our reliance on connected devices continues to grow. The cloud has unearthed a new way of storing, transmitting, and accessing data, and in many ways, it has helped further lay the ground for another trend that has added to the intricacy of the current cybersecurity landscape: The Internet of Things (IoT). IoT devices have been widely commercialized and adopted by the public and use has crossed over into the government sector.

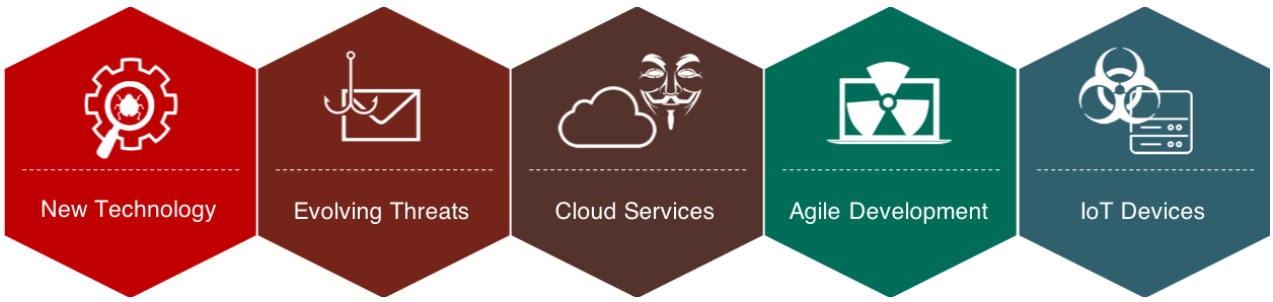
Today, the government is quickly integrating IoT technology into everything from environmental control efforts and natural disaster monitoring to traffic control and power supply. Between 2004 and 2015, the government spent $35 billion on IoT, $9 billion in 2015 alone. A recent study by Gartner predicts that by 2020, 20.4 billion IoT devices will be online, leading to IoT devices outnumbering the global population of users. Though the technology shows extreme promise for future connectivity and management of government and civilian needs, the increasing demand for IoT enabled

products has led to a booming production of low-cost hardware, often devoid of the regulations, certifications, and validations that are required to maintain data security.

This exponential growth and the sheer volume of IoT devices creates a seemingly endless web of connectivity but often at the price of limited visibility and poor manageability – the perfect breeding ground for cyberwarfare at the national and global level. This myriad of devices adds to the network complexity. This complexity should be managed by consolidating as many devices a possible to use the same API. The poor manageability and visibility; along with added complexity, leaves networks at risk.

Agile development has replaced outdated Software Development Lifecycle methodologies, like the waterfall approach. Unlike past methodologies, agile development accommodates frequent shifts or changes in product development and allows for early product delivery, ongoing improvements, and rapid and flexible response to changes and vulnerabilities. The importance of this transition is evident in increased use of agile development across U.S. Government IT projects. Since 2012, there has been a steady rise in major federal projects that self-characterized as either agile or iterative – in 2017, roughly 80% reported as having used these methods according to an analysis of ITDashboard.gov by Deloitte.

When it comes to custom-developed solutions for agencies, agile has its share of downfalls. It often represents an unforeseen pain point for procurement; implementing a solution prone to adaptive change, beneficial as it may be, comes with a unique set of challenges. The same Deloitte report indicates that federal solicitations are requesting roughly the same number of projects to abide by agile development as the waterfall method. There is also the added strain that each agency faces as it implements these changes and comes to grips with facing the unknowns associated with agile: user requirements, design, schedules, and of course costs. For Government procurement of Commercial Off the Shelf (COTS) products, product certifications must still be addressed. As new and more frequent releases come to market, each release must ultimately complete government validation – creating a delay in product availability for procurement. The result is a tradeoff between the need for speed and the need for third-party validation.



GOVERNMENT REACTION & IMPACT

To address the rising concern over growing threats and advancements in technology, the U.S. Government has implemented a variety of policies and mandates to help mitigate risk at both the national and civilian level. Awareness of the following five mandates and policies can equip federal workers with the knowledge needed to prepare for cyberwarfare, protect critical infrastructure, and standardize the approach to securing individual external networks.

- **CNSSP #11** - Released by the Committee on National Security Systems (CNSSP) in 2013, CNSSP 11 was written to address the acquisition of information Assurance (IA) and IA-Enabled Information Technology (IT) Products. This policy dictates purchasing requirements for all U.S. Government departments and agencies, stating that all U.S. Government agencies may only purchase products that have been placed on NIAP's Product Compliant List (PCL) and products that achieve FIPS 140-2, whenever a product includes cryptographic functions.

- **Executive Order 13800 and the Cyber Security Framework** - Issued in 2017 by the President of the President of the U.S., the Executive Order (EO) 13800 on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure effectually dictates that executive department heads are entrusted with ensuring cybersecurity risk management efforts are in place.

  Additionally, the EO mandates the use of the Framework for Improving Critical Infrastructure Cybersecurity Framework (CSF), which was developed by the National Institute of Standards and Technology (NIST). The CSF provides a methodology to assess risk, both internally and externally, and the cyber security of IT infrastructure. The CSF emphasizes the importance of starting with the identification of current systems, assets, data, and capabilities. Identification is followed by steps to protect assets and detect changes and possible cybersecurity events.

- **Risk Management Framework** - Designed to help federal agencies manage the risk associated with information systems and data, the Risk Management Framework (RMF) specifies the implementation of security controls within an agency's system development life cycle. Compliance to the RMF is optional for the private sector, but federal agencies are required to comply as a result of the Federal Information Security Modernization Act of 2014.

- **The Continuous Diagnostics and Mitigation (CDM) Program** – CDM which is consistent with guidance from NIST, is designed to provide the Department of Homeland Security and other federal agencies with the capabilities, resources, and tools to efficiently identify cyber security risks on an ongoing basis. Additionally, CDM provides a structured methodology that allows for risk prioritization based on perceived impact, with the goal of mitigating the most significant risks, flaws, and bugs first. Ultimately, CDM can provide a means to address and react to threats as they occur, which will decrease vulnerability and mitigate the risk of network exploitation.

- **Trusted Internet Connections Initiative 3.0 (TIC 3.0)** - Originally developed in 2007 with the goal of limiting the number of access points from government networks to the public internet, the TIC 3.0 aims to reduce and consolidate external access points, manage security requirements for Security Operating Centers (SoCs) and Network Operating Centers (NOCs), and establish compliance programs that will monitor TIC adherence. TIC 3.0 will also focus more on helping agencies make risk-based decisions and give agencies more flexibility in how they apply the TIC requirements. It's anticipated that TIC 3.0 will lead to decreased implementation times and stronger integration of cloud services by allowing government agencies to utilize those technologies that have already been approved through FedRAMP.

SMART PROCUREMENT & MITIGATING RISK

As technology, threats, and the regulations that govern them evolve, so does the complexity of procurement, creating concerns over how to identify and implement solutions that are as adaptable as they are secure. In today's IT market, it's imperative that those responsible understand how to select solutions that address agency needs and mitigate risks without sacrificing mission critical resources:

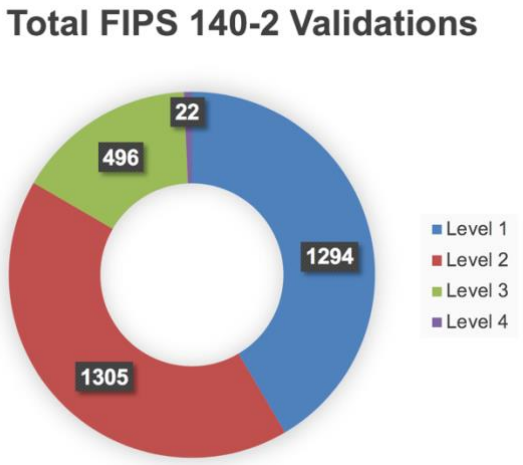
1. Stay on Top of Emerging Standards, Policies, & Mandates

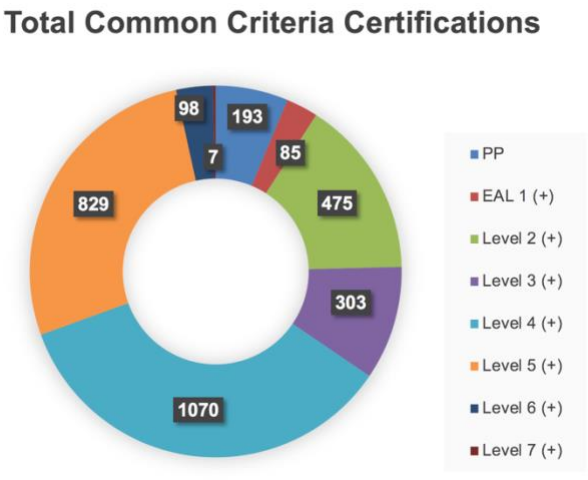
Identifying and analyzing potential solutions that fit agency needs and come with the appropriate certifications and validations is one way to mitigate risk, but to avoid pitfalls that impact mission critical resources, it's essential to stay informed on the latest trends in policy and implementation regulations. Those tasked with procurement authorization are urged to keep the following industry updates and resources in mind as they procure, implement, and maintain a chosen solution.

Emerging Changes	Impact
TLSv1.3	Transport Layer Security (TLS) is a protocol that manages and secures communication between web browsers and severs. Many solutions implement both TLSv1.1 and TLSv1.2. In 2018, TLS v1.3 was finalized – which could impact the longevity of products that utilize outdated versions.
NIST & CMVP Guidance	NIST and the CMVP consistently provide guidance on how to use, treat, and trust approved products as well as re-evaluation requirements. Additionally, both organization provide guidance for federal procurement in the form of best practices, processes, and check lists.
CVE	The Common Vulnerabilities and Exposures (CVE) list catalogs what products have reported and recognized vulnerabilities and exposures that must be addressed to maintain product security and integrity. Those responsible for long-term management of implementation must keep track of what products are implemented or procured on a given network and, if it is on the CVE, then they must respond (e.g., patch, release update, etc.).
FedRAMP	FedRAMP is a government-wide program that provides federal agencies with mandatory guidance on security assessment, authorization, and monitoring with regard to cloud products and services. Both the FIPS and CC communities are working to determining the best evaluation process for products in the cloud and will likely offer guidance on the chosen path, which will impact procurement and implementation.
GDPR	Though the General Data Protection Regulation (GDPR) is a data protection law specific to the European Union, it can impact any organization (public or private) that handles data for individuals living within the nations that make up the EU and can represent the global concerns that, in certain circumstances, must also be considered during the procurement process.

2. Only Purchase Approved Products

Government mandates demand implemented solutions undergo rigorous hardening, testing, and certification/validation. However, to increase the efficiency of the procurement process, preliminary review can be guided by and subsequently narrowed down by identifying products and service providers that have obtained government certifications and approval through an evaluated program, such as FIPS 140-2 validation, Common Criteria certification, or listing on the DoDIN APL. The number of products being certified and validated has steadily increased over the past 20 years. Over 3,100 products have now received a FIPS 140-2 validation and over 4,000 have received a Common Criteria certificate.





Purchasing validated products and services allows agencies to offload security testing and validation to a central certification entity that makes security testing their primary focus. While agencies should not assume that all certified products are secure, purchasing certified products and services provides increased assurance in the product's security posture.

3. Evaluate Certificate Achievement Methods

Though purchasing a solution that has been certified or validated is a proficient step in the right directly, it does not automatically indicate the products and solutions are secure. Not all products that receive federal certifications provide the same level of assurance in their cyber security posture – FIPS and Common Criteria are not simply a "checkbox" along the procurement journey. There are certain factors that can empower procurement offices to immediately prioritize solutions and eliminate those that may not suit the needs or security expectations of the agency. Each office must consider the scope and depth of the evaluation performed on the product or service. This requires government agencies to understand the level of cybersecurity assurance that is provided by the validation path chosen by the vendor.

Both FIPS 140-2 and Common Criteria allow product vendors to select an evaluation boundary that could include the entire product or could include only a part of the overall product. Government agencies must review and understand the scope of the evaluation selected by the product vendor. The scope of the evaluation can be verified by the publicly available documents produced for each certification type.

- **FIPS 140-2 Validation Scope -** Federal agencies are required to use FIPS 140-2 validated cryptographic modules for all Secret, but Unclassified materials. A FIPS validation signifies a vendor has pursued an evaluation based on a cryptographic boundary they have chosen. All cryptographic functions must be performed within the FIPS validated module and must meet all the federal requirements.

  "FIPS Inside" or "FIPS Compliant" indicates that the product vendor chose to implement a FIPS-validated subcomponent (sever blades, crypto chips, software libraries, etc.) and then make the claim that the solution uses FIPS-validated cryptography. A FIPS Inside module is dependent on the priorities of the third-party vendor. If the module validation expires or is revoked, the solution that implements it also falls victim to the weakened or relinquished assurance claims.

  Federal Agencies must read the public documentation that accompanies proof of validation, available on the CMVP website (i.e., Security Policy) and do a side-by-side comparison on what security requirements were tested and what environment the solution was tested in, determining if aligns with the intended deployment.

- **Common Criteria Scope -** There are different paths to achieve a Common Criteria (CC) certification. Vendors can choose to define the functional requirements that the product must demonstrate (an Evaluation Assurance Level or EAL) or conform to a defined set of requirements for their product type (a Protection Profile). Both Evaluation Assurance Levels and Protection Profiles represent viable certification paths.

  Because vendors have the option to choose their path government agencies need to make sure they understand what security functions were tested during the CC evaluation. The CC certification provides assurance only for the functions that were tested. The Security Target document, available on the Common Criteria Portal defines the boundary and the certification level for every Common Criteria certified product.

CONCLUSION

As technology and threats evolve alongside one another, the procurement of products that protect sensitive data and eliminate risk is more important than ever. The shifts and changes in technologies have left government agencies, businesses, and citizens vulnerable to data breeches that can cost billions of dollars and create long-lasting damage, the magnitude of which many agencies and consumers are still trying to determine.

To meet the challenges of this new era of technology, companies like Ixia, a Keysight Technologies business, have recognized the importance and need for secure network solutions within the Federal and private sector. Ixia has developed network visibility solutions like the Net Tool Optimizer (NTO) 7303 and the Vision ONE solutions.

The NTO, a part of the Ixia NTO 7300 chassis family of network packet brokers (NPBs), provides end-to-end network visibility across physical and virtual networks. With flexible and powerful functionality including traffic aggregation, filtering, secure socket layer (SSL) decryption with data masking, deduplication, and intelligent packet management help manage, analyze, and secure networks. The NTO has completed both FIPS 140-2 Validation as well as Common Criteria certification, for more information on these certifications, please review the associated credentials – FIPS Certificate #2983 & Common Criteria Certification.

Ixia's Vision ONE is a turnkey device that enables organizations to maintain security as well as identify and resolve performance problems across physical and virtual infrastructures from a single platform. These solutions help fight against threats hidden in encrypted traffic and also feed data to the right forensic solution. Vision ONE is a crucial step toward complete network security and has completed FIPS 140-2 validation Level 2 and Common Criteria, for more on their certifications, please review the associated credentials – FIPS Certificate #2982 & Common Criteria Certification.

Federal agencies must work hand in hand with solution provides to procure products that have risen to the challenge of meeting rigorous government policies, mandates, and certification guidance. With a focus on deploying advanced threat mitigation strategies, innovative network protection solutions, and sound procurement methodologies, both the private and public sector can reduce the number of security incidents and breaches while overcoming global cyberwarfare attacks.

An increase in network visibility and data protective solutions is no longer an enterprise nicety, but a necessity.

Keysight Technologies, Inc., is a leading technology company that helps enterprises, service providers, and governments accelerate innovation to connect and secure the world. Keysight's solutions optimize networks and bring electronic products to market faster and at a lower cost with offerings from design simulation to prototype validation, manufacturing test, network optimization, and cloud environments. In April 2017, Keysight acquired Ixia, a leader in network test, visibility, and security.

For more information, visit www.ixiacom.com/solutions/network-visibility

Government Checklist to Address Network Visibility:

- ✓ Update outdated monitoring processes
- ✓ Implement secured and validated tools & solutions
- ✓ Optimize data connectivity
- ✓ Use solutions that improve overall performance of monitoring tools