



High performance. Delivered.

The Secure Enterprise
Network Consortium: Helping
Provide Comprehensive Cyber
Security Approaches for High
Performance

• Consulting • Technology • Outsourcing



Cyber Security and the Current Landscape

Our defense networks are under continuous attack. Every day, nearly six million events test our defenses, collect information and try to disrupt our operations. While this is not new, the nature and extent of cyber threats are changing. More and more, cyber attacks are beginning to find their way into warfighting doctrine.

History shows that warfare is dictated and dominated by those who adopt technology advancements to their advantage. Each nation must take notice and act on the growing threat of cyber and kinetic attacks that are designed to achieve political aims. Nation states, organized crime, organizational insiders, malicious hackers and curious savants around the world are strategizing how to steal vital intelligence, cut off information access, spread disinformation and cripple the ability to respond. Equally

threatening, cyber terrorists are working at a pace of innovation that is poised to outstrip the ability to stay ahead of their threats.

Such threats are widespread and diverse. Age-old exploits have been applied to new online systems like the Supervisory Control and Data Acquisition (SCADA) systems that are embedded into critical infrastructure. Other intrusions may have little visible impact, but they enable attackers to learn how an organization's defenses respond. The events in 2007 and 2008 in Estonia and Georgia show how easy it is to bring scale to the cyber fight. In these cases, the expert few quickly reached the curious masses, infected the unknowing and spread their base of operations globally in only a matter of days—cutting off access to banking and government websites. In addition, counterfeit hardware has been inserted into previously trusted systems, resulting in a tremendous volume of identity theft.

Mounting an effective cyber security defense against this breadth of threat is considerably more demanding than staging attacks, in terms of both resources and cost of preparation. It must achieve a very high success rate to be effective. With the clock ticking, nations cannot wait to get out ahead of this challenge.

The Comprehensive National Cybersecurity Initiative

A generation of government and commercial information technology security specialists has been waging a battle against perpetrators. These adversaries readily take advantage of advancing technology to stay in front of defenses, and their attacks continue to increase daily. Dealing with this growing threat has become a national security priority, which has resulted in the creation of the Comprehensive National Cybersecurity Initiative (CNCI).

Figure 1. The Secure Enterprise Network Consortium (SEN-C) assembles capabilities from leading providers of cyber security solutions

	Accenture	CA	Cisco	Los Alamos National Lab	Sun
Situational Awareness	Dashboard Services, R&D	Compliance SW, R&D Services	Resilient Network Solutions		Secure SOA Products
Risk Management	Strategy & Risk Services	Risk Management Software	R&D Services		R&D Services
Analytics	Security Monitoring & Management Services, Managed Services	Analysis & Correlation Software	Network Monitoring & Management Software	Basic & Applied Research and Development	Secure MLS HW/SW Solutions
Telemetry and Health		IT Management Software		Transferable IA IP Portfolio	Identity & Access Management Software
Attributes and Relationships	Identity & Access Management Services & Solutions	Identity & Access Management Software	Network Access Software		Open Source Solutions
Identity					

Despite this priority focus, the effectiveness of the response is still far from ideal. Those on the frontlines of the cyber security battle have inconsistent methods, training, doctrine and tools to do their jobs; there is no common operating picture to enable the strategic level; and there is ongoing competition over who owns the resources—and hence the fight. The National Institute of Standards and Technology, the U.S. Department of Homeland Security and the U.S. Department of Defense have taken strides to improve the odds, but threats are trending in a direction that will likely outstrip the ability to combat them successfully.

Recognizing the challenges of this struggle, the president's IT budget request for the Department of Defense (DoD) for fiscal year 2009 addresses cyber security. It puts fiscal muscle behind fighting cyber threats by infusing the issue into the DoD's four broad areas of focus. The CNCI and the

need for robust cyber security solutions touch every aspect of this IT mission:

Information Age Transformation.

Enabling the DoD, intelligence community and state, local and commercial communities with information capabilities to securely collaborate without information compromise.

Net Centric Data Strategy. The secure discovery, accessibility, stewardship, exchange and targeting of data through dynamic communities of interest so that information consumers can perform individualized modeling, analysis and decision making.

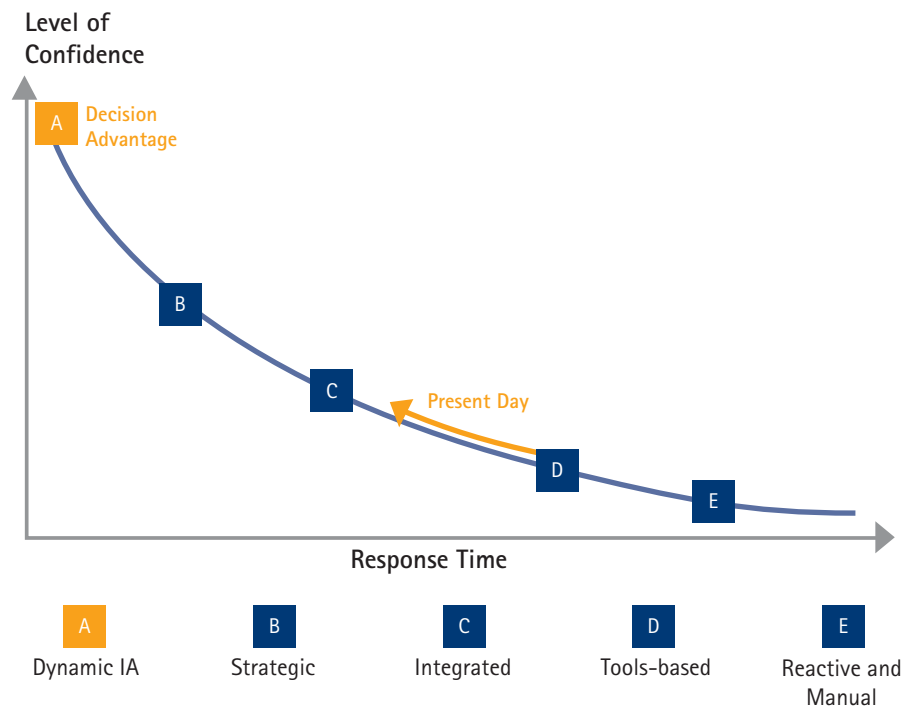
Enterprise Service-Oriented Architectures. Employing open standards and system interoperability to provide methods that any application across the community can use to discover or exchange information, execute capabilities or tap into the vast virtual capacity of the Global Information Grid.

End-to-End Information Assurance (E2E IA). The critical link between the CNCI and the DoD focus areas, E2E IA lays the foundation for trust throughout the entire enterprise through dynamic information assurance capabilities that secure data through its valuable lifespan and through the services and applications that exploit it.

An information assurance groundwork

The 12 initiatives of the CNCI lay a framework for addressing the recognized need for the US government to take decisive action on E2E IA. Coalescing around the CNCI is an important continuation on the journey started with the early steps in cyber security over the past 10 years. Most significantly, it instantiates a philosophy of balancing security with mission capability so that the shared goal is higher operational capability assured by security, not at the expense of or at odds with assuring security.

Figure 2. The SEN-C is committed to helping achieve decision advantage



E2E IA lays the groundwork for safely and securely improving mission success, while keeping pace with information technology and threat advances. The ability to collaborate, understand and act is only as good as the trust in people, information and systems. It is imperative to get that groundwork right and keep it on course with the mission and desired outcomes.

End-to-End Information Assurance is one of the greatest challenges facing the DoD today, and it is the primary focus of this document and the Secure Enterprise Network Consortium. This is the largest cyber security issue facing the DoD and large-scale changes are required to adequately address this issue.

The Secure Enterprise Network Consortium

To help the US address its cyber security needs, Accenture spearheaded the creation of the Secure Enterprise Network Consortium (SEN-C), a

collaborative group of industry and government organizations. The members of the consortium—Accenture, CA, Cisco, Sun Microsystems and Los Alamos National Laboratory (LANL)—bring depth of experience and a diverse set of capabilities and perspectives (see Figure 1). The group is structured around a framework of commercial agreements, as well as a Cooperative Research and Development Agreement (CRADA) with LANL, linked together by Accenture as a systems integrator.

Combining capabilities for superior results

The consortium's goal is to promote interaction and collaboration with the government to develop innovative and comprehensive solutions for cyber security. The result is a set of capabilities and assets that together exceed those of the individual members and help agencies achieve high performance through cyber security.

The consortium recognizes that current and future cyber security needs will not be met solely by existing, standalone products and today's business models. The consortium has a long-term commitment to improving critical infrastructure security for the country and decision advantage for the warfighter. SEN-C's goal is to improve the timeliness of cyber security responses while boosting the enterprise's confidence that the responses have the desired impact (see Figure 2). SEN-C members look forward to identifying cyber security gaps with government input and addressing them with an agile research and development strategy fueled by cooperative efforts between both individual and government cooperative efforts.

With the diverse backgrounds of the consortium members, the combined potential is impressive—and unprecedented. The products, systems integration and true collaboration



offered by the SEN-C represent a history of outstanding achievements in meeting security demands. Team members were selected based on their past achievements in security innovation, their potential for contributing to development of new approaches to cyber security challenges and their record of prominence in providing services for the government:

Accenture. Accenture is a global management consulting, technology services and outsourcing company, applying its information assurance assets, proven delivery methodology and extensive research on the world's most successful organizations to help clients become high-performance businesses and governments. Accenture helps lead complex transformations to successful outcomes by aligning business processes, technology change and organizational shifts toward the desired vision for cyber security.

CA. CA brings expertise in complex IT environment management, information assurance luminaries and a fluid independent research and development capability, drawing on numerous patents for monitoring, managing and securing devices, networks and applications to support the information assurance mission with an integrated system view that recognizes interdependencies and maps technologies to reduce risk. CA supports this effort with more than 5,300 engineers at multiple facilities around the world. CA is also a recognized leader in setting strategy within the Information Technology Infrastructure Library versions 2 and 3.

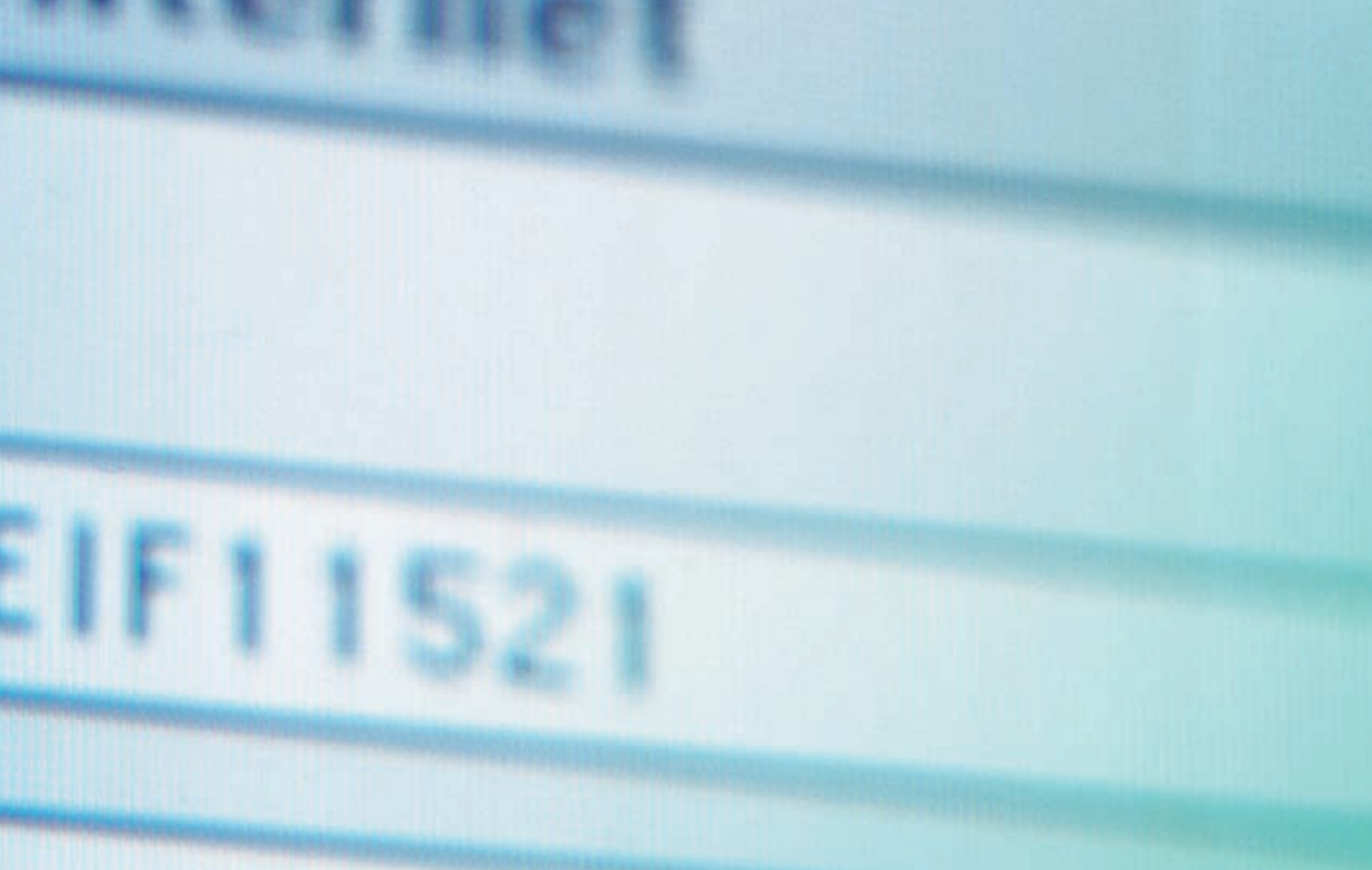
Cisco Systems. Cisco brings leading security that provides rapid response to today's threats and integration for a holistic, self-defending network. The security operations and research and development teams provide early-warning intelligence, threat and vulnerability analysis, and proven Cisco mitigation solutions to protect networks.

Sun Microsystems. Sun brings a combination of information assurance luminaries, trusted software and hardware and strong perspectives and experiences with open source software.

Los Alamos National Laboratory. LANL is a premier national security research institution delivering scientific and engineering solutions for the nation's most crucial and complex problems, filling leading roles worldwide in basic and applied scientific research and technology and bringing a scientific approach to cyber security problem solving. SEN-C members are executing CRADAs with LANL which are centered on CNCI initiatives.

SEN-C Recommendations

Working closely together and with the input of colleagues across the government, SEN-C members developed critical recommendations that can accelerate the journey toward high performance through E2E IA and satisfy CNCI objectives. These collective



insights provide a basis for future discussion, and demonstrate how the SEN-C can assist the government with meeting the CNCI challenge.

1. Push security to enable access and information sharing

The CNCI recognizes that for DoD to succeed at its mission, it must improve information dominance—increasing access, collaboration and exploitation capability—while building security at the very core. This should not be a tradeoff. Rather, security should be an enabling capability, not a barrier. When security is built into the fabric of the enterprise, the applications and user services can expand and improve, demonstrating that trust and protection are built in.

Making security-enabled access a reality starts with some key building blocks:

Security services. The emergence of standards such as SAML and WS-Security, paired with new flexibility around Web Ontology Language

(OWL) for more fluid and interoperable credentialing, creates opportunity to better control the “Wild West” of security services and start coalescing around the right reusable enablers for enterprise security through SOA.

Multi-Level Security enablers. Even early multi-level security (MLS) solutions show promise for compartmentalizing risk while enhancing user access to the information and sources needed to do an effective job. These solutions can couple with SOA approaches to enable an MLS enterprise where preexisting applications can leverage the services to become MLS enabled and extend their useful lifespan.

Security Common Operating Picture (S-COP). Inconsistent adherence to standards, incompatible security models and one-off configurations make it difficult to have a single S-COP across the enterprise. Extracting security policies, helping to facilitate compliance with enterprise standards and rolling up application intelligence to an S-COP

will move the enterprise a long way toward centralized management over decentralized controls and execution.

Access anywhere. Workers need to be connected outside of the office or base, across locations and in the field. They need to share information in untrusted environments to truly achieve the mission and enlist the help of state, local and tribal agencies. And this need is forcing new requirements for mobile solutions. Misplacing these devices can lead to both the breach of sensitive information as well as public outcry. At the same time, creating homegrown solutions that protect the data, but come at several times the expense of commercially available products, draws the same concern. Emerging classes of device management solutions provide robust capability that mitigates risks and enables the flexibility the mission requires.

In short, expanded capability with security at its heart creates new opportunities for success.

The cyber security fight requires leadership and execution by people who have years of experience.

2. Lead cultural change

The biggest disconnect between the way DoD has demonstrated success in the past and how it will need to provide leadership in this current struggle is the cultural journey it will need to take. The guiding tenet here is to focus on outcomes, rather than to manage requirements. Set the bar high, and then manage the journey to reach that outcome.

This new journey looks very different from the large system procurements of the past. There is a cultural shift that needs leadership and it centers on:

The people with the talent to win.

The cyber security fight requires leadership and execution by people who have years of experience. Public service agencies often have a hard time retaining this premium talent and commercial companies are fighting it out on the open market as each guru becomes available. There is a need for new hybrid models where the career proposition is more of a shared benefit for all involved. With that, the United States is vastly under gunned on cyber security talent. It is also difficult to believe that putting a warfighter through six weeks of training will

enable them to immediately succeed as a cyber warrior. Instead, there is a need for a consistent set of capabilities for all future cyber warriors to adopt across the DoD, along with its commercial counterparts, so that the rules, tools and schools for cyber security are consistent and shared.

The community that supports the United States. To augment the talents in the cyber fight, DoD must connect silos of capabilities by aligning that premium talent and giving them a place to share their experiences and collaborate as part of a large, decentralized team. This especially includes the need to collaborate across trusted and untrusted environments. The classified information assurance talent needs to contribute and participate in the larger cyber security activity in the public domain, both to solve their problems as well as cultivate the next generation of talent. The US government needs to engage the broader community for collaboration, resources and capability—more than just listening to the wires.

The way solutions are sourced. The DoD must rethink its development and acquisition strategy. With respect to IT, the current, lengthy procurement strategy leads to a final product that is often obsolete when finally delivered due to technology advances and threat changes. In IT procurements, there should be an outcomes-focused process that allows for concurrent research, development, testing and evaluation. This should be inserted in the development and acquisition process so that at a minimum, the process achieves the stated outcome alongside the latest technology and threat advances. Once this outcome is realized, DoD can work on a development and acquisition strategy that will allow it to be ahead of both future cyber threats and the latest technology during future IT procurements.

High performance through cyber security relies 100 percent on the ability to manage this journey, to be successful in transitioning to

an adapted culture, on changing the way goals are set and revisited, and on fundamentally embracing a discipline counter to today's defense establishment culture.

3. Continuously explore innovative solutions

Numerous solutions exist in the commercial space, others have been custom grown in the defense environment and still more are cropping up all the time in entrepreneurial pockets across the country. The DoD needs to assume a posture where it can quickly adopt a new capability whatever the source, deftly tailor new capabilities to its needs and smoothly integrate new solutions into the larger security picture.

The challenge is not to develop an end state, but to instead resolve a goal and keep moving the bar higher for the community so that it is continually just out of reach. Some of the key opportunities for innovation that the SEN-C has identified include the following:

Enterprise Security Management (ESM). Currently, ESM solutions do an excellent job correlating events across the network as gathered by the sensors deployed throughout the enterprise. But the desired outcome of ESM is to have complete visibility into the activities and their impact going on across the enterprise. In order to do that, ESM must go beyond detecting attacks or logging events and start integrating knowledge about asset availability and performance as well as human behavior threat tendencies and the fusion of logical and physical events. Enterprise security controls should account for operational processes in addition to achieving their security objective. They should be designed and deployed in a manner that enhances manageability and usability and adapts to the mission. Unlike large, monolithic solutions, component-based enterprise security holds promise for achieving both the operational mission

and the information assurance goals with flexibility and interoperability as the guiding principles.

Resilient, self-defending, self-healing networks. A key element for supporting those security controls and enhancing enterprise network security and availability will be the design and deployment of resilient, self-defending and self-healing networks. As we race to build up the competency of the next wave of cyber warriors, commercial and public service organizations have a lot to share and collaborate on for the research to bring these self-healing networks to fruition. They need to pursue training for the human operators and develop decision support techniques to make them even more effective in parallel.

Transmission over untrusted infrastructure. Rapid response to global events will dictate the need for trusted information to run over untrusted infrastructure. There are several efforts underway to provide a trusted layer over untrusted infrastructure, but there also has to be a challenge to look at the utility of the information and determine which option is right for the operating constraints of a particular mission. Examining the timeliness of the information, the content itself and its proposed collection and dissemination points weighs into whether or not to secure it over untrusted capabilities.

Proactive countermeasures. There are technical, legal and geopolitical barriers that must be addressed in developing effective and proactive countermeasures. Some commercial companies already are wading into the gray areas of defending their assets with countermeasures. But the ability to maneuver in the network to both defend and attack is purely a function today of what capabilities a cyber warrior has on their desktop. In the world of cyber security, code is maneuver and every arm in the fight

needs consistent access to the right tools and intelligence to act in the best interest of the enterprise.

These areas compose just some of the innovations that DoD can explore and drive with its commercial partners so that it is not locked into any one custom provider as the cyber security bar moves higher.

Creating strategic alliances to enhance security solutions

Alliances are essential to Accenture's top goal of helping clients become high-performance governments. Accenture extends its technology and business capabilities through a powerful alliance network of more than 150 market leaders and innovators to provide clients industry-leading specialized skills and tailored solutions.

In today's competitive environment, Accenture understands the importance of working with other industry leaders to provide clients with the best possible service. Accenture has teamed with companies such as Sun Microsystems, Cisco Systems, Microsoft, Akamai and Symantec to offer clients proven, measurable and sustainable solutions to meet their security challenges.

Toward high performance in cyber security

The formation of the SEN-C—and the recommendations members have developed together—reflect a unique, industry business model to address the CNCI and the critical cyber threats inherent in today's defense and intelligence environment. The focus is on bringing leading skills together—from thought leadership and solution development to systems integration excellence—to collaborate with government and achieve outcomes that enable CNCI initiatives and improve the nation's security.

For more information about the Secure Enterprise Network Consortium, or about achieving high performance through cyber security, please contact C. Eric Warden at +1 703 947 2986 or charles.e.warden@accenture.com.

Appendix: Secure Enterprise Network Consortium Members

Accenture

Accenture's Security group helps clients build secure and profitable relationships with customers, teammates and constituents while improving business results. Skilled Accenture professionals help government and commercial organizations secure data and protect identities, address threats and vulnerabilities, and meet stringent compliance demands while reducing costs and increasing profitability. Accenture's strategic alliances with world-class technology providers extend our capabilities, reduce project risk and help streamline the vendor evaluation and procurement process. Several Accenture security and information assurance assets and capabilities were developed with or apply technology from SEN-C members, including:

Cisco Solutions Unit (Cisco). Skilled resources focused on Cisco technology and network security.

Strategic Alliance Agreement (CA). A cooperative program that provides CA solutions, training and integration services for clients.

Mammoth Initiative (Sun). SOA and identity management solutions, accelerator toolkits, integration connectors, code samples and

starter packs for rapid and efficient deployment of solutions.

Accenture Multi-Domain Access Solution. A Trusted Solaris Ultra Thin Client workstation capable of displaying data from multiple independent networks at different classification levels, based on the clearance level of the user. This workstation uses cross-domain solutions that are common criteria certified technologies to create accredited multi-level security architectures.

The Accenture Smart Identity Solution. Based on Sun technologies, provides a preintegrated solution for strong authentication, identity management and HSPD-12.

Research and development framework. A Cooperative Research and Development Agreement with Los Alamos National Laboratory (LANL).

CA

CA, founded in 1976, is one of the oldest and largest software companies in the world. Its techniques were the precursor to the Information Technology Infrastructure Library (ITIL); the company holds numerous patents for monitoring, managing and securing devices, networks and applications. CA designs Enterprise IT Management (EITM) solutions to deliver critical situational awareness over the IT infrastructure.

CA is committed to advancing technology research in strategic areas. Through CA Labs, CA collaborates with academia, professional associations, industry standards bodies, customers and partners to explore novel products and emerging technologies. CA spends \$700 million annually on research and development for more than 400 products. A large portion of this spend is focused on supporting third party technologies, including those of the other SEN-C member organizations. CA Labs conducts advanced research in areas related to enterprise IT management, including:

Systems management. Network, systems, database, applications and Web infrastructure

Storage management. Backup and recovery, archiving and compliance

Security management. Identity and access management, antivirus, firewall, anti-spyware, intrusion detection and secure content management

Governance, risk and compliance. Portfolio, service, change and IT asset management

Software development. Advances in computer science and software engineering

Cisco Systems

Building on a history of security innovation, Cisco provides a powerful suite of leading security products, including market-leading firewall, virtual private networking (VPN), intrusion prevention system (IPS), network admission control (NAC) and e-mail security technologies. Cisco security services follow a lifecycle methodology to design, implement, operate and enhance secure networks that are resilient and reliable, and align technology investment with business strategy.

The Cisco Self-Defending Network combines leading point technologies to address and autonomously respond to emerging threats. It encompasses:

Network and endpoint security. Integrates firewall, VPN, IPS and other security services into network devices and endpoints to create an integrated, adaptive and collaborative defense system.

Content security. Extends network defenses beyond the traditional network perimeter to protect data in motion, incorporating e-mail, Web interactions, instant messaging systems and other applications that require content inspection and control.

Application security. Provides protection to applications and data, providing XML and HTML inspection capabilities and fine-grained application control.

System management and control. Integrates sophisticated policy, identity and reputation services with powerful enforcement capabilities. These technologies unify disparate network, endpoint, content and application security services, and provide businesses with unprecedented visibility and control.

Sun Microsystems

Sun has long history of success in working with commercial and government customers to enhance information security and assurance. Sun's existing products include built-in hardware encryption support in a number of server and storage products; solutions for encryption across the network, on disk and on tape; and a full suite of identity management and service-oriented architecture software. Sun maintains a cadre of trained security services professionals who offer advanced experience and services for security assessment, security policy, security engineering and security architecture services. Sun's existing credentials and offerings include:

Sun's government Secure Network Access Platform (gSNAP)[™] architecture builds on Sun's Trusted Solaris architecture to enable simultaneous access to multiple networks, displaying information from each in a separate (labeled) window. Sun gSNAP has been successfully piloted at the Joint Intelligence Center of the Pacific (JICPAC) and forms the backbone of ship-board telecommunications security for the U.S. Navy's new Littoral Combat Ship (LCS) systems.

The Accenture Multi-Domain Access Solution, an Accenture asset, is built on a Trusted Solaris Ultra Thin Client workstation.

Sun and Accenture jointly developed and sold numerous secure SOA and secure identity assets.

Sun's Global Command and Control System (GCCS) delivers integrated products and services that form an integral part of the DOD's GCCS Command and Control architecture and infrastructure elements of the Defense Knowledge Online program (a subset of DoD's Network-Centric Enterprise Services, NCES).

Sun solutions are certified in NIAP, IPv6 and other DoD standards.

Los Alamos National Laboratory

Los Alamos National Laboratory (LANL) is a premier national security research institution, delivering scientific and engineering solutions for the nation's most crucial and complex problems. Los Alamos National Laboratory personnel play leading roles worldwide in basic and applied scientific research and technology. LANL has received 107 prestigious R&D 100 awards for technologies with commercial promise since 1978.

LANL computer security leadership is long-standing. In 1984, Wisdom & Sense was the first anomaly detection system to generate rule-based profiles of normal activity. In 2007, Packet Analytics received venture funding to commercialize network forensic search engine technology developed and deployed at Los Alamos. LANL is a leader in quantum cryptography and computing and holds the distance record for quantum key distribution.

LANL's current network security focus is on enabling technologies to make networks resilient in the face of persistent internal and external threats. Resiliency includes the concepts of fault-tolerance, survivability and self-healing network systems. The Global Virtual Vault project is pioneering ways to control the threat of insider theft of information and removing the need to secure data stored on desktop and mobile computers. LANL leverages ubiquitous network connectivity to move all media, data storage and computing out of the user's environment and into secure data centers. By controlling communication at this level, LANL removes the reliance on cumbersome client management requirements such as data encryption and port controls and enables access by untrusted partner, coalition, or personal computers and smartphones.

Copyright © 2009 Accenture

Accenture, its logo, and High Performance Delivered are trademarks of Accenture

All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. This document is for your informational purposes only. To the extent permitted by applicable law, this document is provided "As Is" without warranty of any kind, including, without limitation, any implied warranties of merchantability or fitness for a particular purpose, or non-infringement. In no event will any party be liable for any loss or damage, direct or indirect, from the use of this document including, without limitation, lost profits, business interruption, goodwill or lost data, even if the parties are expressly advised of such damages..

About Accenture Defense

Accenture's Defense industry group provides leading services and methodologies that help departments of defense, the intelligence community and federal agencies achieve high performance in support of the warfighter. The addition of mission services to Accenture's consulting, technology and outsourcing offerings means that clients can meet future goals, mitigate risk and realize cost savings. Visit www.accenture.com/defense for more information.

About Accenture

Accenture is a global management consulting, technology services and outsourcing company. Combining unparalleled experience, comprehensive capabilities across all industries and business functions, and extensive research on the world's most successful companies, Accenture collaborates with clients to help them become high-performance businesses and governments. With more than 186,000 people serving clients in over 120 countries, the company generated net revenues of US\$23.39 billion for the fiscal year ended Aug. 31, 2008. Its home page is www.accenture.com.

