TSCP
Executive Interviews

TABLE OF CONTENTS

TSCP would like to thank **Deloitte & Touche, LLP**, a TSCP Member, for its dedicated work in conducting the executive interviews, facilitating the executive session and producing this white paper.

TSCP
EXECUTIVE INTERVIEWS

I. Executive Summary

In 2014, TSCP published its ***Transglobal Security Collaboration Program Strategy: 2014-2016***. TSCP is in the process of reviewing and validating the strategy as well as updating its priorities and deliverables for 2017-2020. As part of this process, the Leadership Advisory Group consulted with member executives to ascertain their positions and opinions on key developments and challenges facing the security environment in the Defense IT industry. Member executives also were asked what role TSCP should play going forward in supporting a common approach to resolving these challenges. In addition to the interviews, executives and the Leadership Advisory Group participated in a facilitated session to discuss the results and provide additional input. The results and recommendations will be used as the starting point for updating goals and objectives for the revised TSCP strategy. This white paper presents the results of the interviews and facilitated session.

TSCP Strategy & Accomplishments. The first part of this paper summarizes TSCP's mission, vision, strategic principles and goals. TSCP's strategic goals and objectives are centered on enabling and demonstrating secure collaboration and information sharing between industry and governments in the Defense IT community through the development, promotion and adoption of interoperable specifications based on common standards that facilitate compliance, thereby minimizing the costs to individual members. This section also enumerates TSCP's recent accomplishments, i.e., publications, outreach activities, demonstrations, leadership initiatives, new memberships, and special interest groups.

Member Industry Trends. The second part of the paper presents executive responses to trends in key industry topic areas: Security/Cybersecurity & Identity, Emphasis on Data, Defense Agencies' Focus, IT Investments, Cloud Migration Challenges, Proliferation of Mobile Devices and What Keeps You Up at Night?

In general, the executive interviews highlighted that the Defense IT community has shifted its focus on establishing the groundwork for identity management to a focus on deploying access management, in other words, usage. Over the last 10 years, TSCP members and customers have deployed and integrated identity management systems, issued strong credentials and established the foundations for interoperability. Now they are working to strengthen authentication, add authorization and deploy federation and secure access to resources across the community environment. Within the U.S. DoD, for example, identity management is slowly migrating to a centralized enterprise service across applications, which should facilitate the transition from a program-by-program approach to a more holistic approach to identity and access management. Over the last two years, there has been a particular emphasis on the protection of data and Intellectual Property through the employment of data tagging and labeling linked to identity and access control across the Defense IT community.

Executives also reported that in the last several years the Defense IT infrastructure has been expanding because of increased information sharing across business partners and will continue to expand with the explosion of mobile devices and cloud computing. While member companies' defenses have improved, the supply chain has become the preferred point of entry for many security breaches. As a result, TSCP members and customers continue facing the risks associated with internal and external cyber threats and are working to deploy security controls that prevent breaches rather than remedy them after the fact. Identity and access management plays a key role as a foundational tool for cybersecurity.

The Defense IT community faces significant budget cuts that are expected to continue over several years. This should increase TSCP's value proposition as it promotes common approaches and standards that leverage and reuse, which results in cost savings.

TSCP Focus 2017 & Beyond. The third part of this paper focuses on the role TSCP can play going forward in assisting with common approaches to resolving the challenges. Topic areas include: Projects and Capabilities, Customer Requirements, Strategies and Approaches, Areas to Address in the Future, Business Development and Education and Training.

Executives recommended that TSCP expand the marketing of its specifications and capabilities, specifically in the areas of identity credentialing and the secure exchange of data. In addition, TSCP should develop approaches to privacy protection and data exchange across international lines. Going forward, executives recommended that TSCP deliver a set of specifications and services that address commercial applications, e.g., financial services verticals.

To extend the value delivered to its members, executives recommended that TSCP increase the involvement of the business area representatives in the early phases of the work product lifecycle development process. Also, in this era of limited customer budgets, TSCP must be more selective and customer-focused in the projects it selects. To broaden adoption, TSCP should focus on alignment with established standards and best practices and strengthen its relationships with the procurement community. Finally, executives recommended that TSCP apply the successful formula of targeted position papers, such as the DoD Relying Party Paper, to similar critical issues for leadership action.

Over the next several months, the results and recommendations from the executive interviews and facilitated session will be used as the starting point for updating priorities, plans and deliverables for 2017 and beyond.

II. Introduction

In the Defense IT community, secure collaboration depends on the ability to share information across its stakeholders – governments, contractor companies and their supply chains – while at the same time complying with multi-national jurisdictions. Having established a common framework that enables secure collaboration and assured information sharing across the Defense IT community, TSCP has created an environment in which the stakeholders can operate effectively, efficiently and securely while performing on programs. Focusing on these activities through a consortium of stakeholders facilitates standardization and interoperability across the community.

Thus, the TSCP community works together to solve common challenges that impact major programs today: mitigating the risks related to compliance as well as the complexity, costs and duplication inherent in large-scale, collaborative programs that span national jurisdictions. TSCP members face common issues and understand the advantages and savings that can be gained through collaborating on the challenges of secure information sharing. TSCP has developed and practices an industry approach to protecting sensitive information based on interoperable trust mechanisms.

TSCP is in the process of reviewing and validating its strategy as well as updating its priorities and deliverables for 2016-2020. As part of this process, the Leadership Advisory Group consulted with member executives to determine their positions and opinions on key challenges facing security in the Defense IT industry and, in general, to reveal what is “on their minds.” Member executives were asked what role TSCP can play going forward in assisting with a common approach to resolving these challenges. In addition to the interviews, executives and Leadership Advisory Group members participated in a facilitated session to discuss the results and provide additional input during the TSCP Executive Committee Meeting on October 4 in London. The results and recommendations will be used as the starting point for updating plans. Given the number of extensive responses, the Leadership Advisory Group will devote several planning sessions to studying and prioritizing the recommendations.

This white paper is presented in three parts:

- TSCP Strategy & Accomplishments
- Industry Trends
- TSCP Focus 2017 & Beyond

III. TSCP Strategy & Accomplishments

To place the interview responses in context, a brief recap of TSCP's existing strategy is presented in this section, which includes TSCP's mission and vision statements, current strategic goals and principles, as well as a summary of its accomplishments to date. (TSCP's complete strategy, including objectives related to goals, is available for download at the www.tscp.org.)

3.1 Key Strategy Elements

TSCP's mission and vision statements are as follows:

MISSION: TSCP is a cooperative forum in which leading Aerospace and Defense (A&D) companies and key government agencies work together to establish and maintain an open standards-based framework that can be used to enable secure collaboration and assured information sharing between parties, irrespective of the tools they choose to use.

VISION: TSCP will migrate from serving as a TSCP Member resource to serve as the authoritative source for secure collaboration standards in the Defense IT community.

3.2 Strategic Goals

Part of the purpose for conducting these interviews is to determine whether and how TSCP's existing goals and objectives need to be updated or changed. The strategic goals from the 2009-2011 strategy were derived from the mission and vision statements. The full TSCP strategy lays out specific objectives related to each goal. The goals are summarized as follows:

1. **Goal 1:** Enable information sharing within and between industry and governments.
.
2. **Goal 2:** Enable collaboration compliant with export control and relevant policies and company Intellectual Property protection policies.

3. **Goal 3:** Define a set of interoperable specifications and solutions that enables re-use in a cost effective manner across multiple programs.

4. **Goal 4:** Make TSCP specifications and solutions a standard in Defense IT.

3.3 Strategy Principles

TSCP's business drivers are those requirements that compelled Members to unite for a common purpose. TSCP and the Defense IT community at large have a business need for:

- **Collaboration.** Collaborate and share data in program and stakeholder environments typically characterized by fragmented IT systems, tools and processes. Address specific collaborative needs and requirements on government programs.

- **Security.** Address security gaps when collaborating and sharing data and mitigate related risk exposure.

- **Costs.** Minimize duplicative costs on IT utilities and infrastructure used for collaboration.

- **Compliance.** Comply with government policies, regulations and standards that impact secure collaboration across international and company borders (export control, IT security, identity verification, data sharing, data access rights, etc.).

3.4 ACCOMPLISHMENTS TO DATE

TSCP has established a strong coalition of IT Defense industry leaders to address common challenges facing the stakeholders in key government programs. TSCP has produced the following:

Publications

- Trust Point magazine
- Next version of Secure E-mail Specification (authentication based on labeling)
- Information Labeling and Handling Specification
- US, UK, and Dual Use Export Control Requirements for Secure Collaboration
- White paper to spur increased usage by Relying Parties for the Federated PKI Infrastructure
- Identity Federation Common Operating Rules
- White paper on Advanced Persistent Threat
- Updated / Published TSCP Architecture Design

Outreach Activities

- Engagement with Standards Bodies and Trust Framework Providers to ensure TSCP Alignment
- Participation in UKCeB Secure Encrypted E-mail over the Internet (SEEOTI) Project
- Participation on the Identity Ecosystem Steering Group (IESG)

Demonstrations

- Demo of Identity Federation with NASA and A&D Companies

Leadership Initiatives

- Submitted comments on FIPS 201-2, XACML 3 OASIS Standard, NIST 800-63-1 and DODI 8520.03
- Drove PKI Trust between the US and the Netherlands

New Memberships

- Added new TSCP Members – NATO, NASA, Synergen, CertiPath, FuGen and Electrosoft

Special Interests Groups

- Hosted a Special Interest Group (SIG) for Access Control
- Hosted Forums for Identity in the Cloud, Mobile Computing, Access Management and Identity Federation
- Hosted webinars on information protection and access management

IV. Member Industry Trends

The section that follows describes the executives' responses to questions designed to elicit their opinions and recommendations related to key topics and challenges facing the Defense IT and security industry today. The bullets under each topic list items from most to least frequently mentioned (in descending order). Because the exercise involved interviews and a free-flow discussion at the facilitation session, this is not a precise priority ordering.

4.1 Security/Cybersecurity & Identity

Knowing who and what are accessing corporate data and facilities is a key tenant of identity and access management. Secure collaboration in cyberspace is facilitated through a seamless and robust identity architecture that is interoperable across participating organizations. ***Executives were asked:***

What are your organization's key objectives related to IT cyber security and identity?

- **Continue to Implement and Step Up Strong Authentication.** Authentication as a means of access has become the norm across member companies. The current focus is on implementing stronger methods and various higher levels of authentication as required for the resources being accessed, and thereby enhancing the security of member programs.

- **Focus on Data Access & Protection.** (See below, section 4.2.)

- **Evaluate/Implement Federation.** Members are in the process of evaluating or implementing federation as a method for extending security out to the members' entire operating environment, particularly within the TSCP community.

- **Close Security Gaps through Identity Systems Integration.** Members are integrating their identity networks, particularly systems that have previously remained outside the primary security domain, including international sites. While this integration yields numerous benefits and economies, from the standpoint of security, it enables members to further centralize security operations and plug security gaps.

- **Secure the Supply Chain.** Members are testing and evaluating credentialing and authentication methods to facilitate secure access of their supply chains to their data and networks. For example, one member is testing a solution in which tokens are used for application enablement for its customers and supply chain.

- **Address Machine Health.** Members recently have begun to address machine health on an enterprise-wide basis. Particularly in an environment where there are scores of mobile devices connected to the infrastructure, members are looking to establish methods and metrics around maintaining machine health across the enterprise as well as to those entities with which the enterprise interoperates.

4.2 Emphasis on Data

Over the last 10 years, Defense IT entities have been focused on identity management, i.e., establishing and validating identities and making them available across their enterprises for the purpose of secure authentication. Going forward, industry participants are now focused on securely accessing data based on this foundation of identity and authentication mechanisms. Key to a successful secure collaboration environment is organizing corporate data across the enterprise in order to consistently label and control access. ***Executives were asked:***

What data management activities is your organization focused on?

- **Data Protection through Classification, Labeling & Tagging.** Currently, and over the last several years, members have expended significant resources around classifying, labeling and tagging data, not only to protect the data itself, but also to isolate the data according to its sensitivity properties and thereby control access to information according to users' roles in their respective organizations (including external entities).

- **Tie Data to Access.** While most members' focus over the last 10 years has been on building trusted and secure identity and access management systems, the focus is now shifting to tying identity and authentication to data to allow for more granular access, particularly in mobile and remote access environments. Are you who you say you are? What systems do you have access to? What data are associated with your access rights?

- **Migrate to Multi-Level Security (Europe).** Many Europeans governments and the members with whom they do business have migrated to a multilevel security environment. To facilitate the exchange of data between networks and environments, confidential and sensitive data is segmented and secured while still allowing access to less sensitive data in order to conduct day-to-day business.

- **Organize Data for Analytics and "Views".** Governments are starting to address organizing and formatting data/data stores in a manner that facilitates data analysis, detection of anomalies and offers flexibility in the way data can be viewed and analyzed, particularly for Defense and law enforcement agencies.

4.3 Defense Agencies' Focus

TSCP's primary constituents and customers are the Defense agencies of their host countries, e.g., US DoD, UK MoD and Netherlands MoD. They are the entities with which TSCP members companies effectively interoperate and collaborate securely. ***Executives were asked:***

What initiatives and requirements are Defense agencies focused on?

- **Security Requirements for Mobile.** Defense agencies continue to develop requirements and evaluate security solutions for mobile devices. Security in the mobile environment is at varying degrees of development and also varies by the type of device. For example, US DoD has secure solutions for PCs and Blackberries, but not yet for iPads and other mobile phones. However, there are still no standards for a classified data spill; at this point, a data spill associated with a mobile device can only be remediated by destroying the device. (And, what happens if the device is stolen or lost?)

- **Security Requirements for Cloud Computing.** Outside of private cloud environments, existing security protocols for cloud are insufficient for high threat environments (such as Defense programs). Although Defense agencies are successfully implementing cloud in closed environments and using it to virtualize their own systems, they are waiting for security specifications for "open" cloud to be significantly strengthened before it is widely adopted for Defense programs.

- **Access Technology for Collaboration.** Defense agencies have "done" identity management and are now focused on access management, i.e., establishing various levels of authentication and access rights to networks, systems, applications and data in order to create an end-to-end trusted environment.

- **Deploying Tools for Secure Collaboration.** In order to effectively implement access technology, Defense agencies are deploying tools for secure collaboration. Given the somewhat fragmented chain of command in Defense IT departments, the challenge is and has been to get the application owners in the various agencies to embrace and implement collaboration tools.

- **Migrate from Program-by-Program to Holistic Approach to Identity Management.** Historically, Defense agencies have been accustomed to managing resources on a program by program basis. For security reasons, and for many of the program-specific functions, this has been the most effective way to manage large Defense programs. Identity and access management, on the other hand, is more secure and efficient when managed in a consolidated manner and is certainly required for a collaborative environment. Therefore, Defense departments have been working towards expanding the scope of authority of the IT departments to build common solutions and drive consistency across agencies, based on holistic requirements and on an information architecture approach.

4.4 IT INVESTMENTS

The global economic situation continues to stress IT investments, particularly in the areas related to cybersecurity. In an era of budget cuts and uncertainty in terms of future revenue levels, member organizations have been required to exercise prudence and scrutinize expenditures. ***Executives were asked:***

What IT investments will your organization be making related to secure collaboration and cybersecurity over the next 2-5 years?

- **Data Labeling Implementations and Rights Management.** As members collaborate across corporate and national boundaries, consistent labeling and marking of information is critical to protecting proprietary information and complying with export control policies. Members are engaged in the joint development of common specifications that address information protection.

- **Federated Access Implementations.** Federation is a critical component for secure collaboration across organizations. Members continue to work with TSCP to develop access applications that protect and facilitate secure data access across organizational boundaries with industry issued tokens such as smart cards, Common Access Cards (CAC), PIV cards and PIV-I cards.

- **Implementation of Secure Email Exchange (TSCP).** Avoiding one-off solutions and using industry standards enhances members' return on investment (ROI) by creating solutions that are reusable by many programs, thereby reducing overall operational and maintenance costs while protecting content during transmission and storage. Members are exchanging email securely with customers, partners and suppliers by encrypting the content, many through the use of TSCP Secure Email specifications.

- **Stepping Up Strong Authentication.** Members are stepping up efforts around deploying strong authentication, e.g., using smart cards and certifying them to the Federal bridge.

- **Security/Privacy Controls/Measures to Prevent Hacking & Increase Usability.** Members don't want to follow the concept that "security just happens." Security controls have to be developed with usability in mind – enterprises cannot require difficult or complicated procedures for end users. At the same time, members are working to constantly stay a step ahead of hackers trying to breach their environments. Members are working on establishing security programs focused on prevention and anticipation of security vulnerabilities and risks, rather than addressing breaches after they have occurred.

- **Continued Protection of Intellectual Property.** Members continue to be concerned about and address the protection of Intellectual Property, which largely led to the aforementioned IT investments.

- **Continued Identity Systems Integration.** Members are focused on integration of identity systems to plug security gaps and maximize the trustworthiness of the identities and related credentials.

- **Further Deployment of PIV and PIV-I/Medium Hardware.** For government agencies (US), deployment of PIV continues to be a high priority. Government agencies are now promoting the deployment of PIV-I/medium hardware to interface to state, local and the private sector, particularly in the finance and critical infrastructure sectors.

Gold (Technology) Members were specifically asked about the solutions and capabilities they are currently developing and plans for the next 2 to 5 years.

CA Technologies Investment Focus

- Strong authentication, with particular attention to mobile device
- Granular access management tied to data
- Increased use of partnering, outsourcing and data sharing
- Policy-based secure email solution

Microsoft Investment Focus

- Building policies around data classification into the applications themselves (policy-based automation)
- Capability is already available with Outlook and Word

4.5 Cloud Migration Challenges

Cloud has been billed as the solution to collaboration over the Internet. The on-demand nature of cloud computing potentially offers economies of scale, lower costs and fast deployment of applications to the Defense IT community. TSCP members are assessing migration to cloud to take advantage of these benefits and to increase the ease of sharing data and accessibility of resources. The openness of the cloud environment, however, comes with security challenges. ***Executives were asked:***

> ***What IT and program challenges are your organization facing related to migrating to cloud computing?***

- **Security & Data Protection for Cloud.** Members and their customers/key decision makers express concerns when it comes to storing highly sensitive information in the cloud. (See above, *Defense Agencies' Focus: Security Requirements for Cloud Computing*.). In a cloud environment, they perceive a loss of control over the endpoints and are concerned over how to secure them.

- **Need for Initial and Ongoing Risk Assessment.** Because of the fluidity of data movement in the cloud environment, member IT departments will need to perform risk assessments with increased regularity, strengthen monitoring functions and develop capabilities to address remote repair capabilities (e.g., remote wiping of devices). Historically, governments and members often have evaluated cloud services from a cost-savings standpoint, rather than from a risk assessment perspective.

- **Protecting and Managing Identity in the Cloud.** Having successfully established identities and managing them across their networks, members are turning their attention towards protecting, securely authenticating and generally managing identities in the cloud. Given the efficiencies, cost savings and security associated with PKI and web communications, as well as the ability to

circumvent storage of identity information in a few data centers, security in the cloud may, in fact, have the potential of being more secure than using conventional approaches.

- **Policy Development and Enforcement in the Cloud.** Over time, security policies have developed around the existing model of on-premise IT with extended access via the web. In preparing for migration to a cloud environment, members are facing the challenge of developing and enforcing policies in a manner that is suited to this new environment.

- **Private vs. Open Cloud.** For governments, a private cloud approach allows governments to protect the privacy of their citizens, businesses and partners. For the time being, many governments (US and Europe) are setting up systems in closed/private cloud environments until such time that security on the open cloud is proven.

- **Law Enforcement in the Cloud.** Recognizing that major portions of IT systems will migrate to the cloud, law enforcement agencies are concerned about and starting to address how to track data in the cloud environment; conducting data forensics in the cloud is much more complex than in the conventional IT environment.

Gold (Technology) Members were specifically asked about what solutions and capabilities are being developed related to cloud computing.

- **Enablement for Cloud.** Technology members are working on robust, secure and fast solutions for the cloud and are enabling existing services (e.g., collaboration) for the cloud. They are addressing related issues such as how data will be handled and stored, privacy, security and reporting.

- **Efficiency around Cloud.** Technology members are developing solutions that leverage but protect the data collected in and across organizations. Although cloud technology unleashes the movement of data across organizations, members now have to look beyond how they currently store and permit access to and build collaboration bridges while protecting against information leakage. Particularly in a government environment, citizens and businesses give governments and companies a great deal of sensitive and confidential data that has to be protected.

- **Identity Management in the Cloud.** Technology members are developing consolidated cloud offerings that manage identities, e.g., federated single sign-on (SSO) for cloud and cloud-based strong authentication.

4.6 Proliferation of Mobile Devices

Over the last 10 years (and particularly in the last 5 years), IT organizations have been facing a proliferation of mobile devices that need to be integrated into their organizations' infrastructures. In addition, the "consumerization of IT" has resulted in the pervasiveness and intrusion of social media as well as users and employees bringing their own devices (BYOD) into the workplace with the expectation of having them connect to their work IT networks. ***Executives were asked:***

What impact do you see mobile devices having on secure collaboration in your organization? What are the challenges?

- **Security and Functionality for Mobile Devices.** Currently, security for mobile devices is relatively ineffective and still emerging; current solutions are "klugey." Members generally agree that more of the core requirements need to be integrated into the devices and well tested before member organizations will be willing to consider completely replacing laptops and desktops with mobile devices.

- **Diverse and Rapidly Changing Technology.** Not only have the numbers and types of mobile devices proliferated over the last several years, but the technologies on which they are based have been constantly changed and improved. The most recent challenge is the trend to bringing your own device (BYOD) to the workplace. Members IT departments are facing the challenges associated with continuously integrating and securing these devices into their infrastructures as well as updating security policies accordingly.

- **Economics of Adding Mobile Devices to the Infrastructure.** Until and unless member organizations are able to replace users' laptops and desktops with mobile devices, they face increased expenses rather than cost savings. This will take time – in addition to the issues cited, mobile devices are not as secure or effective as existing devices for running multiple applications.

- **Coexistence with Social Media.** Although an important new tool for collaboration, the explosion of social media - often accessed through mobile devices - has had a direct impact on member organizations' ability to secure their data and infrastructures. Member organizations are finding themselves having to address hacks and scams that penetrate their infrastructures through social media. Not only are they working on developing detection and protection techniques, but they are also in the process of instituting social media policies.

- **Need for Initial and Ongoing Risk Assessment.** As with the introduction of any new application or type of device into an organization's infrastructure, when considering a mobile deployment, a full risk assessment needs to be conducted and the identified risks must be addressed. In the ever-changing nature and variety of mobile devices, however, members are beginning to recognize that risk assessment will need to be an ongoing process.

- **Need for Continuous Monitoring.** As a follow on to the need for ongoing risk assessment, members noted that continuous monitoring may be the most appropriate solution in a mobile environment. Mobile devices almost need to be considered as external devices due to their vulnerability and must be continuously monitored for potential risks and breaches.

4.7 What Keeps You Up at Night?

In addition to addressing specific and timely topics, member executives were asked about general challenges they face in today's and tomorrow's IT security environment. ***Executives were asked:***

What IT security and cyber challenges and risks are coming down the road? What keeps you up at night?

- **Proliferation of Mobile Devices that Need to be Secured.** (See above, section 4.6, *Proliferation of Mobile Devices*.)

- **Insider Threats: Intentional & Unintentional.** Government respondents see a strong opportunity to leverage TSCP capabilities using private sector resources to develop cutting edge solutions that will improve and protect the infrastructure from internal threats (both intentional and unintentional). They recognize that employees are the first-line of defense. Thus, a major area of concern lies in the use of social engineering tactics to effectively target employees, which makes sensitive information, IP and PII data vulnerable to breaches.

- **External Threats and Related Costs.** Members continue to deal with ever-mutating threats and tactics used by adversaries (countries, companies and individuals) that sell offensive services. Members are now being forced to budget and expend more funds and resources to deploy new defensive solutions and advanced forensics capabilities than in the past.

- **Location and Protection of Data in Cloud Environment.** Because identifying the location and security of an organization's data in a cloud environment is vastly different than the traditional concept of location-based data and control, members are concerned about how they will maintain control over and secure their data in cloud environments. (See above, *Cloud Migration Challenges*.)

- **Inherent Weaknesses in COTS Solutions.** Member IT infrastructures consist of a combination of COTS solutions, both hardware and software, that often have exploitable security gaps. Rather than "fix" these security gaps once the solutions are deployed, member organizations are starting to address these vulnerabilities with COTS developers at the source before delivery and integration into their infrastructures.

- **Control of Information Security/IT Hygiene.** Members contend that there is no "silver bullet" for security, but rather a combination of processes is necessary: keeping patch levels up to date, network monitoring, securing access, strong security policies, etc., i.e., IT hygiene. The constant pace of technology development is not going to stop – members expressed the need to establish security approaches/processes that adapts to the new and accelerated pace of technology.

- **Compliance with Policy & Mandates.** Polices and mandates that flow down both from government and from member organizations often need to be "automated" through IT applications and the infrastructure. Members are facing the challenge that the accelerated pace of cyber threats has resulted in a similar acceleration of policies and mandates that are continually filtered down to the IT department, often with short timeframes for implementation.

- **Uneven Economic Equation in Cyberspace.** Members are facing a progressively lopsided economic equation in cyberspace, i.e., it is easy and lucrative to be in the "bad" group (hackers, exploiters, etc.) and increasingly difficult and more expensive to be in the "good" group. More and more actors with nefarious intentions are building capabilities to do bad things to TSCP members' critical infrastructures. Having to constantly develop countermeasures is very expensive.

V. TSCP Focus & Beyond

TSCP has developed and practices an industry approach to protecting sensitive information based on interoperable trust mechanisms. Having established a common framework that enables secure collaboration and assured information sharing across the Defense IT community, TSCP has created an environment in which the stakeholders can operate effectively, efficiently and securely while performing on programs. Focusing these activities through a consortium of stakeholders facilitates standardization and interoperability across the community.

Member executives were asked specifically what role TSCP can play going forward in assisting with common approaches to resolving the challenges that emerged from the interviews. The Leadership Advisory Group will use the results and recommendations that emerged from this process as a starting point for its updated strategy and will work to prioritize activities going forward. TSCP focus areas are:

- Projects and capabilities
- Customer requirements
- Strategies and approaches
- Areas to address in the future
- Business development
- Education

5.1 PROJECTS & CAPABILITIES

TSCP's work on new capabilities, publications and specifications is managed through the TSCP project lifecycle process. The TSCP Leadership Advisory Group sought the input and recommendations of members executives regarding what projects and capabilities the working groups and committees should pursue going forward. ***Executives were asked:***

What should TSCP's focus be for projects and capabilities?

- **Develop Approaches to Privacy Protection and Data Exchange across International Lines.** TSCP should develop a common approach to the protection of privacy and data exchange that will be acceptable and achieve compliance across its international communities.

- **Complete Labeling and Digital Rights Specification.** After the TSCP data labeling specification is completed, TSCP should extend and translate it into an interoperable digital rights capability. The fundamentals of labeling has to be perfected first; TSCP then needs to focus on information exchange across the major TSCP participating countries, i.e., a core set of standardized information exchange specifications.

- **Extend and Market Federation.** Although TSCP has successfully demonstrated and uses federation across its membership, the capability has not extended much beyond the membership. TSCP should deliver and promote a set of federation protocols that industry can and would want to adopt.

- **Establish Standardized Structure for Implementation and Follow Through.** TSCP should develop a standardized structure for implementation of its specifications and capabilities, possibly by establishing a formalized TSCP reference architecture. This approach could provide members with the opportunity of producing and procuring a consistent set of solutions.

- **Deliver First Set of Services and Standards that Address Commercial Applications (Verticals).** TSCP's secure collaboration capabilities strongly converge with capabilities required by its members, however, the broad implementation of TSCP-based solutions within member companies and programs is taking longer than anticipated. In addition to its existing programs, TSCP should look to vertical commercial applications and industry groups to achieve faster adoption of its specifications.

- **Develop Provisioning Application Model & Authorization Standards.** TSCP should develop a provisioning application model that enables members and industry to perform provisioning in a consistent manner.

- **Map NATO Restrictive Credentials to PIV and PIV-I.** In order to expand interoperability of secure information exchange internationally, TSCP should initiate a project that maps NATO restrictive credentials to PIV and PIV-I specifications.

- **Explore Opportunity in Attribute Management for Government Transactions.** The Defense/ government IT and PIV/I communities recently have elevated the imminent need for stepping up authentication through the use of attributes in a federated environment. Having been approached by the Government members and its Defense IT supply chain, TSCP should explore the role it should play in the governance and/or operations of an attribute exchange broker for the government market.

5.2 CUSTOMER REQUIREMENTS

The Leadership Advisory Group is particularly interested in understanding what member executives are hearing from their customers in terms of goals and concerns that could impact future TSCP projects. ***Executives were asked:***

What customer requirements should TSCP address over the next 2 years?

- **Need for Cyber-Educated Workforce.** On a global level, one of the most critical customer challenges is the shortage of qualified candidates to fill cybersecurity positions. TSCP should address approaches for filling vital cyber jobs, e.g., malware analysts, penetration testers, system administrators and computer scientists.

- **Secure Collaboration through Standards-Based Federation in the Cloud.** More and more, customers will be pursuing federation solutions in the cloud. TSCP should extend its existing federation work to achieve secure collaboration in the cloud.

- **Decrease the Need for Regulation through Common Solutions.** Standards and regulations do not necessarily make systems more secure. TSCP should identify and address security gaps through an approach that can ultimately reduce the need and burden for additional regulation.

- **Promote Policies for PIV-I-Based Federation.** A key customer objective is to achieve interoperability with their governments. TSCP should continue to study and address related policies and actively engage governments to continue advocating minimum requirements for identity cards that can be trusted and accepted by governments, in particular, the US Federal Government PIV-I.

5.3 STRATEGIES & APPROACHES

In addition to recommendations on specific projects and capabilities, the Leadership Advisory Group is interested in how TSCP can improve on the strategies and approaches that are used to perform, organize and execute on its work. ***Executives were asked:***

To continue providing value to its members, what strategies and approaches should TSCP employ going forward?

- **Get Business Side Involved in Lifecycle of Work Product Development.** TSCP's broad mission is to deliver value to its customers and members. TSCP should focus more attention on ascertaining current and future requirements from the government customer's point of view. TSCP's business representatives need to be more involved in the decision process for identifying the projects and capabilities TSCP will pursue. The resulting work products will likely produce a more favorable ROI for both governments and company members.

- **Develop Marketing Strategy.** TSCP should develop a cohesive marketing strategy that targets key customer stakeholders to promote TSCP's value proposition.

- **Be Selective on Projects, Sharpen Focus and Accelerate Deliverables.** TSCP members' and customers' investment streams have become more and more limited because of budget restrictions; TSCP must be selective and prioritize the projects and capabilities it will be pursue. In addition, because of the overall acceleration and ever-changing nature of technology development, TSCP should accelerate the rate at which it produces deliverables.

- **Align TSCP Solutions to Standards.** Members recognize that major cybersecurity challenges cannot be solved through regulation. By the time any useful laws/regulation would get through the government process, the technology and threat will have already changed. TSCP should line up

its products/services with established standards (such as NIST 800-53, etc.) to demonstrate that the use of TSCP-based technology lowers risk.

- **Drive Towards Open Standards & Best Practices.** When developing its projects and capabilities, TSCP should continue to drive towards open standards and best practices.

- **Apply "Formula" of DoD Relying Party Paper to Similar Issues of Concern for Leadership Action.** TSCP should build on the success of DoD Relying Party paper and apply the same formula to other key issues, for example, authentication for mobile devices. This approach will help strengthen the links and collaboration between key TSCP representatives and their government counterparts and put them in a position to help governments with guidance on policy from the private sector perspective.

- **Anticipate the Future/Next Generation IDM.** TSCP should be asking the members and customers about future important issues that will need to be addressed, e.g., the next version of IDM, authentication, etc. TSCP engineering working groups should be task-oriented about solving these challenges. This approach could be powerful in anticipating government procurements.

5.4 Areas to Address in the Future

In addition to near-term projects, capabilities and requirements, the Leadership Council solicited recommendations on areas TSCP should address further into the future. ***Executives were asked:***

What areas should TSCP address in the future that will provide value to the members?

- **Develop Standards around Identity Governance.** Identity and access management is an established function in the IT Defense industry. In the not too distant future, TSCP should focus on the critical need to establish governance around identity management. In this context, identity governance refers to the management of access rights and requests and roles-based access to reduce the surface area of access weak points.

- **Start Addressing Commercial Market.** TSCP member organizations understand the requirements and solutions for secure collaboration and data exchange better than most segments of the security industry at large. TSCP should start to address and play in the commercial market (i.e., beyond Defense IT and government). If it does not, IT tools and requirements will be driven by Facebook and similar user-based application providers.

- **Develop Approach to Alignment with Government Regulation.** TSCP should develop a software approach to address regulatory and contractual requirements. Regulations and audit are very complex and require a heavy investment of resources; TSCP should develop a deliberate approach for evaluating regulatory requirements and utilize an engineering approach to address them.

5.5 Business Development

The Leadership Advisory Group solicited recommendations on how to encourage adoption of TSCP specifications and capabilities. ***Executives were asked:***

What business development strategies should TSCP employ to increase its value?

- **Establish Relationship with Acquisition Community.** Defense agencies recently have started to reorganize their procurement communities to leverage experience, increase effectiveness and reduce duplication in resources and costs. TSCP should take advantage and establish relationships with the acquisition community and communicate and educate them on TSCP

capabilities thereby increasing the potential of TSCP capabilities being incorporated into procurements.

- **Exert Influence on Community Requirements.** Related to the previous recommendation, TSCP should promote solution paths for implementing capabilities within the customer community in order to increase the likelihood that they appear in RFP requirements. TSCP should focus on uniform requirements for solutions that can have uniform requirements.

- **Reach Out to New Platinum & Gold Companies for TSCP Membership.** TSCP should reach out to new Platinum and Gold companies for TSCP membership in order to extend its ability to establish common specifications that are even more broadly developed, accepted and used.

- **Further Cooperation in Targeting International Challenges.** TSCP should place increased focus on furthering cooperation on projects and capabilities that respond to international challenges, e.g., implementing privacy controls across international lines.

- **Target Speakers to Extend TSCP Understanding.** TSCP should target key customers – e.g., Air Force, Navy, Army, DoD and NSA/NASA – as keynote speakers for TSCP events as a means to educate them on TSCP solutions and value and convert them into TSCP champions.

- **Encourage Government to Play Convening Role.** TSCP's strong credibility lies in its inclusion of government customers and its transatlantic nature. TSCP's should regularly host sessions that bring together government decision makers to share information and discuss challenges and future investments.

- **Facilitate Information Sharing on Cyber Events.** The cyber community continues to suffer from a lack of information sharing related to cyber events from which all participants could learn. TSCP should facilitate information sharing events on cyber incidents in which the identity of organizations will be kept confidential. TSCP should take advantage of the membership of the Secret Service so that the community can identify new ways of alerting on cyber-attacks and malware.

5.6 EDUCATION & TRAINING

The Leadership Advisory Group solicited recommendations on the types of educational tools and materials TSCP should develop for its membership. ***Executives were asked:***

What types of education and training can TSCP produce or sponsor that would provide value to its members?

- **Produce Webinars on Topics of Interest.** TSCP should produce webinars to educate members' customers on best practices, collaboration projects and new technology. TSCP's customers want to hear what other companies and competitors are doing in the area of identity and access management. TSCP should maintain these webinars on its website and also allow members to offer them on their websites.

- **Produce White Papers on Topics of Interest.** TSCP should produce white papers on topics of interest, e.g., federation, handling of protocol, data handling, etc. Members could use these papers as educational tools both internally and with their customers and prospective customers.

- **Develop/Produce Demonstrations on Products & Capabilities.** Members find TSCP demonstrations to be very useful, e.g., the secure email demonstration. TSCP's ability to bring stakeholders together to work on common security problems is extremely valuable and provides

credibility. TSCP should continue to develop demonstrations on capabilities that highlight TSCP specifications.

- **Recommendation: Education on Adoption of Strong Credentials.** TSCP should develop an educational product that provides information on the adoption of strong credentials. Members could use the product for education within their organizations and for their customers.

- **Recommendation: Education on How Users are Targeted in Cyberspace.** TSCP should develop an educational webinar on how users are targeted on the Internet, e.g., by email and malware. TSCP should present related risks and solutions that TSCP is working on for the future. The product should demonstrate assurance in the exchange of information, standards for identification and characteristics of effective software, etc.

VI. Conclusions

TSCP's strategic goals and objectives are centered on enabling and demonstrating secure collaboration and information sharing between industry and governments in the Defense IT community through the development, promotion and adoption of interoperable specifications based on common standards that facilitate compliance, thereby minimizing the costs to individual members. While this overall strategy remains valid, the challenges to which the strategy, goals and objectives are applied have expanded in the Defense IT environment. At a high level, the executive interviews identified trends that TSCP will need to address:

- Members continue to close gaps and strengthen security across their enterprises, partner organizations and supply chains through identity systems integration, federation and stronger authentication. Key areas of concern continue to be compliance with policy and mandates.

- While the last 10 years have been focused on perfecting identity and credential management, members have turned their attention to access control and data management: data classification, labeling and tagging and tying data to access control, i.e., digital rights management.

- Over the next 2-5 years, members will be focusing IT Investments on solutions and tools for enhanced secure collaboration and cybersecurity including data labeling; expanding federated access and further deployment of PIV and PIV-I (medium hardware); and, security and privacy controls to prevent hacking and increase usability. Two key new areas of investment will be implementation and stronger security for cloud computing and mobile devices.

Executives recommend that TSCP implement a process to carefully prioritize and sharpen its focus, in other words, prioritize projects that selectively address these trends in alignment with its mission, particularly in light of ongoing Defense budget cuts.

For TSCP to achieve its fundamental goals of establishing common specifications that are widely adopted within the Defense IT community depends on having a predominant majority that subscribe to its common approaches and specifications. As such, executives advocate further expanding TSCP membership, particularly across the various stakeholder groups so that more and more players are adopting its approach and specifications. Executives also recommend that TSCP develop and implement a marketing strategy that targets key stakeholders, including the acquisition community.

To ensure that TSCP responds to its community's business requirements, executives recommend that TSCP increase the involvement of its representatives who are aligned to business areas, particularly during the early phases of the work product and deliverable development. Because of its success in delivering highly secure and interoperable data sharing, going forward, executives recommend that TSCP work to deliver a set of specifications and services that address commercial applications that value

security, e.g., financial services verticals.

Finally, TSCP's future success will depend not only on continuing to fulfill its core mission, but also on offering opportunities for stakeholders to convene and work through issues, make decisions and take advantage of educational and training opportunities. TSCP should expand its offerings in these areas and extend the opportunities to members, their supply chain and customers.

Over the next several months, the results and recommendations from the executive interviews and facilitated session will be used as the starting point for updating priorities, plans and deliverables for 2013 and beyond.

VII. Executive Respondents

Below is a list of the TSCP Member Executives who were interviewed for this white paper and/or participated in the executive facilitated session.

- **Fekke Baker,** Program Manager, Netherlands Ministry of Defense
- **Colonel Rob Boots,** Civil and Military Collaboration, Netherland Ministry of Defense
- **Major David Butt,** Strategic Cyber Defence Operations & Policy Officer , UK Ministry of Defence
- **Malcolm Carrie,** Director Strategy & Architecture, BAE Systems, TSCP Board Member
- **Jeffrey Brown,** VP & CISO, Raytheon Company
- **Michael Denning,** SVP & GM Security Customer Solutions, CA Technologies
- **Denis Gardin,** SVP CyberSecurity Solutions, EADS
- **Jeremy Grant,** Senior Executive Advisor for Identity Management, NIST, US Department of Commerce
- **Anthony Jones,** Director, Cyber Threat Operations Enterprise IT Security, Raytheon Company, TSCP Board Member
- **Tom Kelly,** Director of Information Security, The Boeing Company, TSCP Board Member
- **Russ Koste,** Director**,** Identity, Intelligence & Network Defense, Northrop Grumman, TSCP Board
- **Philippe Laflandre,** CyberSecurity Solutions, EADS, TSCP Board Member, Chairman
- **Art Lofton,** VP & Chief Information Officer, Aerospace Systems, Northrop Grumman
- **Dr. Douglas Maughan,** Division Director, Homeland Security Science and Technology HSARPA/CSD, US Department of Homeland Security.
- **Tim McKnight,** VP & CISO, Northrop Grumman
- **Chandra McMahon,** VP & CIO, Enterprise Business Services, Lockheed Martin
- **Kevin Meehan,** VP & CISO, The Boeing Company

- **Air Commodore Mark Neal,** CIO, UK Ministry of Defense
- **Greg Roecker,** External Alignment Manager, Lockheed Martin, TSCP Board Member and Vice Chairman
- **Bharat Shah,** VP & GM Online Services Division, Microsoft
- **Peter Woudsma,** Engineer C4ISR Technology Coordination & Demonstration, NATO Allied Command