# Operational Research Consultants, Inc.

# Comments on the Draft Department and Agency Implementation Guidance on Homeland Security Presidential Directive 12 (HSPD-12)

## Introduction

Operational Research Consultants, Inc. (ORC) is pleased to offer the following comments on the draft department and agency implementation guidance on HSPD-12 to the Office of Management and Budget. Under the GSA ACES and DoD PKI programs ORC has worked closely with the Federal Government over the past twelve plus years to address the initiatives concerning Critical Infrastructure Protection, most recently magnified by HSPD-12. We have additionally invested many of our own resources to provide full "life cycle" IA and identity management services. Directly linked to ORC's GSA schedules Federal, State and Local Governments, as well as, businesses and individuals doing business with these entities can find proven and mature enterprise solutions.

ORC is certified by the General Services Administration (GSA) eAuthentication Program Management Office as a Credential Service Provider (CSP) to *facilitate public access to the services offered by Government agencies through use of information technologies, including on-line access to computers for purposes of reviewing, retrieving, providing, and exchanging information*. ORC's Digital Certificate Credentials are authorized to provide trusted individual or business identity information for use by the FirstGov and participating Government agencies. These Credentials can be used to:

- Authenticate to government and organization websites containing Sensitive But Unclassified (SBU) information.
- Contract for the purchase of goods or services
- Verify the identity of electronic mail correspondents
- Verify the identity of web/ application servers
- Verify the identity of individuals accessing data servers
- Verify the integrity of software and documents posted on data servers

ORC's Digital Certificate Credential services include:

- Department of Defense External Certificate Authority[1] (DoD ECA)
- Access Certificates for Electronic Services (ACES)[2]

These certificate authorities (CA's), owned and operated by ORC, issue level 3 and level 4 compliant digital certificates (all employing an in-person vetting process) to agencies, businesses, associations and individuals who wish to conduct electronic business and services with the Federal Government and the DoD[3]. Under these programs, ORC is the only trusted third party authorized to issue Medium Assurance, Medium Hardware Assurance, Server Certificates and Code Signing Certificates:

- Medium Assurance certificates are generated and protected in a software-based cryptographic module (FIPS 140-1/2 level 1) and are intended for applications handling sensitive medium value information based on the relying party's assessment, with the exception of transactions involving issuance or acceptance of contracts and contract modifications.
- Medium Hardware Assurance certificates are generated and protected in a hardware-based cryptographic module (FIPS 140-1/2 level 2) and are intended for all applications operating in environments appropriate for medium assurance but which require a higher degree of assurance and technical non-repudiation based on the relying party's assessment.
- Code Signing Certificates assert a Medium Hardware Assurance and provide trusted verification of the integrity of software and documents.

---

[1] ORC is certified by the Department of Defense as a trusted third party under the DoD Public Key Infrastructure (PKI). The first of three designated, ORC is authorize to issue digital certificates to businesses, associations and individuals who wish to conduct electronic business and services with the Federal Government. ORC has recently been approved as the first External Certificate Authority under the new U.S. Government ECA Certificate Policy. Mandatory for access into DoD and other U.S. Government Business-to Government (B2G) web sites, the ECA offers non-DoD entities the ability to transact electronic business with or for US Government entities. ORC ECA Subscribers include contractors, vendors, allied partners, North Atlantic Treaty Organization (NATO) allies, Foreign Nationals, members of other Government agencies and their trading partners.

[2] ORC is a certified Certificate Authority (CA), by the General Services Administration (GSA), for the Access Certificates for Electronic Services (ACES) program. This program designates ORC as a trusted third party certificate authority to provide digital certificates to the citizenry of the United States. The ACES certificates provide each and every American citizen and business the accepted digital certificate to conduct business electronically with Federal agencies such as the Veteran's Administration, Social Security Administration and any other agency offering services via the Internet. In addition to an the ACES contract, ORC is authorized as a trusted third party to sell ACES certificates directly to the business and private citizen communities.

[3] The DoD has mandated the "use of digital certificates to secure communications and access to DoD systems, by October 2003", attachment (1). While the DoD Public Key Infrastructure (PKI) is rapidly deploying the DoD has also mandated that for the exchange of unclassified information with vendors and contractors "the DoD shall only accept PKI certificates obtained from a DoD-approved external certificate authority (ECA)", attachment (2).

- Server Certificates provide trusted verification of the identity of web/ application servers and enable those servers to support encrypted (Secure Sockets Layer) transaction protection.

ORC is ready today to offer theses comprehensive systems engineered, integrated solutions in aggregate to meet the business processes of our customers and help them attain OMB compliance.

## General Comments

The Government has provided a public focus focused on the requirement to ensure the integrity of sensitive or confidential information a task that is complicated by the fact that the same information to be protected must also be circulated among a limited, but frequently changing, audience. From the Computer Security ACT of 1987 to HSPD-12 we have conceded that sensitive information exchange must be provable who (by name, not simply office) the provider of a piece of information is and it must be provable that no one has modified the information subsequent to its issuance. There must be no question as to exactly when the information was published. There must be a means of reviewing the history of any particular document, in terms of who did what to it, and when, as it was developed and circulated. There must also be a means to archive all information securely as well as a means to recall the information from the secure archive at a later time. The information fog preceding September 11, 2001, recurring virus attacks, and the clutter of spam and porn on the Internet have demanded an urgency to these requirements.

Yet, after years of development and piloting, we continue to delay implementation in lieu of new invention or re-development. We continue to hear from the policy community that the solution to protecting our infrastructure appears to require Herculean effort. However, appearances can often be misleading. This undertaking is achievable, the tools and technology currently exist, and some are already being leveraged by certain government agencies. The systems and technology, develop in partnership with Government and Industry, are easy to use and suitable for senior executives, managers, and workers at all levels. Reliability is very high and supports the mobility of some of its users.

Over the past several years the advancements in the development and production of identity management, digital credentialing, smart card and biometric technologies has seen significant progress. Further, the integration of these technologies into legacy and current generation environments has grown correspondingly. Unfortunately, the policies and acceptance of these technologies have progressed at a much slower pace. To a large degree, this resistance has been due to fears of the loss of privacy and images of “big brother.” Such fears are not without merit. However, such fears do not have to be realized if the approach, polices, procedures and education is proliferated.

Since 1996 properly managed digital credentials have provide the additional security needed to afford all parties a high level of confidence that individuals attempting access to resources are who they claim to be or that the actionee of a transaction can be identified and non-repudiated. Achieved without compromising or infringing upon the privacy of the individual by simply

adhering to established standards, policies and procedures to enforce the proper use and integration of the technologies, and laws to provide the requisite ramifications for transgression.

For nearly as long, cryptographic smart cards have afford an obvious benefit, mobility. By possessing a credential that can authenticate that an individual is who they claim to be, regardless of where they are coming in from, is highly beneficial. This un-tethers the individual from the desktop or laptop and frees them to move from station to station. And because there are such requirements within the Federal Government such a FIPS (Federal Information Processing Standard) to ensure such functionality as the token being tamper proof, for example, among other requirements, the level of assurance can remain consistent. However, with digital transactions smart cards are only as effective as the credential the card is protecting.

Biometrics can now provide a uniqueness of the person's identification, 'something you are.' Advancements have led to the ability to distinguish an individual by their fingerprint, voice, face, eye, entire body, and more. More importantly, devices are being developed that can use multiple biometric 'signatures' to exponentially increase the accuracy of identification and decrease the possibility of a 'false positive' or incorrect identification.

For ten years Federal agencies have been awaiting meaningful and efficient implementation guidance for security into Internet/ Intranet operations to protect sensitive information and billions of dollars in transactions each day, as well as the privacy of its citizenry. Although digital credentials have been available from a certified "trusted third party" recognized and accepted both internally and externally as trustworthy is the front-runner to achieve these requirements, we have come well short of adopting this proven solution and have spend an enormous amount of money "polishing" the policies and "studying" potential enhancements.

Here again, in response to the President's desire to protect our critical resources, we decided to study the problem instead of implementing a solution. The Draft Department and Agency Implementation Guidance for Homeland Security Presidential Directive 12 guidance directs the agencies to meet schedules, write reports and meet some high level requirements. What we should be providing to agencies, re: "How should I implement the directive?" is to implement proven capabilities that the Federal Government has already sunk cost into and enhances those solutions iteratively, as the rest of the software development community does. For example:

1) Implement an identity management process to reissue Government ID badges on Cryptographic smart cards for Physical and Logical access.

- Refer to document "XXX" for card topology guidance.
- Require a background investigation for all new credentials.
- GSA Common Access Cards are available today for implementation. The following cards are approved (refer to GSA GWAC).
- We anticipate a Card technology refresh to be implemented under new FIPS 201 by ....

2) Include approved digital certificates for logical access control. The following PKIs are certified (DoD PKI, US Government ECA, ACES, ....)

- Configure your applications to use the approved digital certificates for logical access. Refer to the GSA ACES PMO and DoD PKI PMO for application enabling guidance and support.
- Implement agency policy to require digital signing of email and documents.
- "Lock-down" of all critical IT resources shall be completed by the end of FY2006.

3) Reallocate your 2005 personnel and security management and IT expenditures to the issuance of the new card configuration and low level logical access controls to establishing a digital certificate enabled environment.

- Refer to the GSA ACES PMO and the DoD PKI PMO for migration guidance.
- Expert engineering and implementation support is available on the GSA ACES GWAC and on GSA Schedule from the following approve PKI managed service vendors.
- Provide OMB with budget shortfalls.

Once adopted, increasingly mature internal and interagency policies can be developed to ensure only those designated as authorized can gain access to resources while facilitating expedited secure communications with partners, vendors and citizens. And, equally important, the advancement of technologies such as smart cards and biometrics can be focused on enhancing existing security tools to ensure to a great degree that the individual presenting his or her self is, in fact who they claim to be. Combined with asymmetric key technology, smart cards and biometrics provide 'three factor' protection of that digital credential.

- Something one knows, (pin or a password);
- Something one has, (smart card); and
- Something one is, (biometrics).

The technologies necessary to attain digital security in our open society are available. Asymmetric credentials fully support non-repudiation and ensure user privacy coupled with multiple levels of credential protection based on the requisite security need. In more simple terms, providing each citizen the means by which they can authenticate themselves using something they know (password), something they have (smart card), and something they are (biometric) can begin today. Further, this does not have to be done at the expense of anyone's civil liberties. However, to do so we must embrace the technology available today and continue to evolve these technologies as advancements emerge and technologies mature. The infrastructure to mitigate much of the risks associated with digital transactions is fielded. With your support, the ACES, DoD PKI, and DoD ECA programs can be embraced to avoid many of the problems that stand in the way of the President's eGov initiatives. Instead of continually reinventing the mousetrap, we need to use the mousetrap we have and continually enhance that trap to remain one step ahead of the mice. Through proper integration and configuration, security can be achieved and inalienable rights protected. Leveraging these technologies is not a panacea. It is an achievable undertaking that will "provide for the common defense, promote the general Welfare, and secure the blessings of liberty to ourselves and our posterity."

## The Goal of Security

Security by definition is "something which guarantees or safeguards". With regard to Information Systems Security, it is defined as: "The protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats". That which is to be guaranteed or safeguarded is primarily the information asset residing within an enclave, enterprise, database, desktop, laptop, etc. Thus, Information Security applies to anyone using a computer, PDA, cell phone, and so on. In other words, it applies to most everyone in American society today.

There are numerous facets to Information Security that wage a continual tug-of-war, such as protection, privacy, availability, and so on. There are also a plethora of less than ethical individuals using malicious code to wreak havoc on their target du jour, as well as the unsuspecting. The news recently was once again filled with reports of viruses and worms spreading to businesses and households alike. To quote a September 1, 2003 article by Chris Taylor of Time magazine, "worms spring from the minds of virus writers, who could be sitting at any computer in the world. Most spread because we do careless things like open e-mail attachments from strangers, but some have evolved to spread through computer networks on their own — like plague bacilli that have become airborne. "

The key piece of Mr. Taylor's article is the statement that "we (people in general) do careless things like open e-mail attachments from strangers". This does not (and should not) have to be the case. The ease with which nefarious code writers proliferate malicious code is a travesty that does not have to be. Still, our Government has not taken advantage of the significant investment already made in digital certificate technology, a technology that can present an enormous roadblock to such worms and viruses as 'Blaster' and the 'I love you' virus, and the like. By embracing this existing infrastructure, transactions that do not originate from an entity authenticated with a credential from a known, trusted authority, can easily be discarded and we will all live to see another digital day.

The target we should all be striving for is to attain the highest level of security, without sacrificing availability to authorized parties, and without encroaching upon the civil liberties under which our country was founded and has operated for over two hundred years. Moreover, it is critical that we all understand that we cannot allow technology to be the driving force behind the policies governing their use. Instead, it must be common sense, sound policies and prudent laws that dictate how technology can complement and augment the safeguards and protections already in place. Too often, a new technology is devised and we make the mistake of compromising our processes and procedures so that the new technology can be used. This is analogous to building a brand new automobile in order to properly accommodate a newly invented radio. If the radio cannot be produced so that it can be integrated with an automobile, it must not be a car radio. If a technology or device requires the comprehensive reconfiguration and reconstruction of the existing resources, policies and procedures, it is not a proper fit.

***Privacy issues***

It is with good reason that most people in the today's society (including Government employees and contractors) are skeptical of a universal identification card that contains confidential information. Or, that they have fears of their personal data residing in a database somewhere that can potentially be 'hacked' into, causing their data to be compromised. Unfortunately, in the haste of the Internet boom vast amounts of personal data were willingly and/or unwittingly made available by individuals themselves, marketing groups, businesses, even some Government agencies, and a whole host of others. Now, we are left with trying to lock-down as much as possible while simultaneously reeling back in that which has escaped. Society's collective sense of being jaded by the Internet is quite well founded. However, the Internet was never intended to afford privacy to anyone. Quite to the contrary, the Internet was devised for the open sharing of information to anyone and everyone with a connection. Nonetheless, this is the state we are currently in, and some measure of privacy is still attainable.

Asymmetric key technology offers both identity assurance and privacy by representing an individual's identity with a key pair. Properly managed, the private key is created and retained by the owner and only by the owner (as is the case with the ECA and ACES programs). The public key is then freely distributed to a public repository(s) where it can be accessed by anyone known or unknown. Despite being based on complex cryptographic technology and high-side mathematics, the user experience is quite simple.

***Implementation***

Federal agencies must lead the implementation of meaningful and efficient security into Internet/ Intranet operations to protect sensitive information and billions of dollars in transactions each day, as well as the privacy of its citizenry. ECA and ACES "trusted third party" digital credentials, recognized and accepted both internally and externally as trustworthy, achieve the President's Critical Infrastructure Protection initiatives, in short order.

Time is of the essence and cost is a factor. Leveraging the Governments investment in proven managed services (such as ECA or ACES) eliminates the lead-time needed to become operational while insufficient implementation guidance encourages agencies to consider in-house development efforts. The heavy lifting has already been done. ECA and ACES enables agencies to quickly deploy a fully operational capability, providing the highest levels of physical and logical identification and authentication of users and devices, securing of sensitive data, time stamping and archiving of data, and an auditable process flow. Further, the credentials used to accomplish all of these requirements are interoperable with any other agency or organization choosing to accept "Federal-compliant credentials". And, of equal or greater importance, because the trial and error phase has been previously facilitated, the resulting answers can be immediately gleaned, thereby mitigating overall costs dramatically.

## About Operational Research Consultants, Inc.

ORC was incorporated March 28, 1991 in the Commonwealth of Virginia. The company's objective is to provide high-quality systems engineering support services to the US Government military and civilian agencies. ORC's first engagement provided Computer Systems Engineering services to the Naval Air Systems Command, the Navy and Marine Corps Intelligence Training Center, and the Naval Supply Systems Command. On August 27, 1993 ORC was certified under the Small Business Administration's 8(a) program and successfully graduated from that program in 2002. ORC is now a wholly owned subsidiary of Widepoint Corporation[4].

While supporting the Navy, ORC was increasingly engaged to enhance the disposition of Sensitive But Unclassified (SBU) information in a digital environment. To address information assurance concerns in a Business-to-Government (B2G) environment, ORC launched the Navy Acquisition Public Key Infrastructure (PKI). This system, which was later adopted as an official DoD PKI pilot program, provide immediate and simultaneous access to secure information throughout the many existing electronic networks of the Naval Systems Commands and their private industry partners. The requirements for both government and private security included:

- Cross-certification with industry and foreign nationals,
- Single-sign-on for secure server access, and
- Secure electronic mail with industry.

While implementing the Navy Acquisition PKI, ORC also developed an architecture called Public Key Enabling Infrastructure (PKEI)©, which integrates critical, standards based tools for access and identification in electronic medium.

ORC leveraged its experiences with the Navy to become one of the nation's premier systems engineering firms with a specialization in *information assurance and security*. This is evidenced by the following accomplishments:

- ORC was distinguished as the first designated DoD Interim External Certificate Authority (IECA-1) and more recently the first US Government External Certificate Authority.
- ORC is distinguished as one of only three GSA Access Certificates for Electronic Services contract recipients.
- ORC is distinguished as the first commercial GSA eAuthentication Service Provider.

[4] WidePoint Corporation (OTC BB: WDPT) is an Information Technology services and solutions firm specializing in planning, managing, and implementing government and commercial business solutions. WidePoint is using a "commonwealth" model for its growth strategy with key management being retained in each acquired entity, and the realization of efficiencies by leveraging resources and personnel. For more information please see WidePoint's website at www.widepoint.com.

- ORC has been engaged as the lead systems engineer for the DoD PKI, which is currently issuing 15,000 to 20,000 Common Access Cards (with DoD certificates) daily.

Based on PKEI©, ORC has migrated this architecture into a Common IA Enabling Infrastructure (CIEI)©, targeting B2G, Government-to-Government (G2G), and Citizen-to-Government (C2G) Enterprise requirements for:

- Secure and trusted identity creation and management;
- Authoritative sources for credentials and entitlements; and,
- Convenient access to Enterprise resources while maintaining appropriate security.

Because of our unique experiences planning, developing, implementing, and maintaining information assurance infrastructures, ORC has a growing niche in the medium to high assurance level market that is based on flexibility. ORC's CIEI© allows enterprise and application owners to begin where they currently are architecturally and migrate toward a vision of a secure network identity model. And, ORC is poised to support these secure network identity enterprise requirements (in-house or outsourced), by providing seamless integration of four services that make up our CIEI©:

- iDentity Management – providing infrastructure and processes that provide for creation and maintenance of an identity, including centralized administration and self-service of user accounts.
- eAuthentication – providing authoritative repositories for identity, network and/or resource profiles combined with security services that enable identification, validation and support for authorization.
- Access Management – providing authorization, audit functions and session management that enable enterprise and application owners to define access rights for individuals carrying out roles such as a business partners, suppliers, customers or employees.
- Provisioning and Workflow – implementing business policies across enterprises, applications and data that support a higher degree of automation (devices such as identity tokens, credit cards, cell phones and personal computers).

ORC's CIEI© and services leverage standards based, mature commercial-off-the-shelf components that have been proven in the technology market, offering the efficiency of a common solution for multiple applications within an enterprise and interoperability with the Federal Government and trading partners. ORC can also replicate these services (in part or whole) to provide an Enterprise the following advantages:

- Enabling organization's applications with multiple I&A/validation interfaces rapidly;
- Enabling enterprise applications to have enterprise or local access to account data;
- Centralizing enterprise configuration management, managing information with multiple authentication methods;
- Enabling local policy to determine trusted authentications by each application (i.e., application does not inherit trust that is not wanted);
- Implementing of components designed to manage specific tasks so that applications do not have to support all authentication functions natively;

- Enabling an easy migration path from less elegant eAuthentication schemes through higher assurance, including full PKI implementations and Federated Identities; and,
- Enabling organizations to leverage a Government approved solution.