UNCLASSIFIED

JOINT STATEMENT OF

JOHN L. OSTERHOLZ

PRINCIPAL DEPUTY CHIEF INFORMATION OFFICER

DEPARTMENT OF DEFENSE AND

NORMA J. ST. CLAIRE

DIRECTOR, INFORMATION MANAGEMENT FOR

PERSONNEL AND READINESS,

OFFICE OF THE SECRETARY OF DEFENSE

BEFORE THE HOUSE COMMITTEE ON

GOVERNMENT REFORM

21 JUNE 2001

UNCLASSIFIED

Government Paperwork Elimination Act

The Department of Defense is committed to achieving the goals of the Government Paperwork Elimination Act (GPEA) within the target of October 2003.

Electronic business or e-government represents the new approach to streamlining and structuring business and processes to meet the global and competitive challenges of the future. Congressional support with legislation such as GPEA, the Clinger-Cohen Act (CCA), and the Government Performance and Results Act (GPRA) provide the foundation for advancing E-Business across the Department.

E-business is an important tool to improve customer service and governmental efficiency through the implementation of improved processes and the application of information technology. Such improvement involves transacting business electronically with the public, trading partners, and other federal agencies using the Internet and its World Wide Web. In so doing, we must ensure the ability to electronically protect individual citizen and employee privacy, the intellectual property rights of our partners, and sensitive DoD information.

Since 1988, the Department of Defense has been on a path to achieve strong electronic authentication of individual employees and the capability to sign digital documents. In 1988, we codified those requirements in the Defense Message System program documentation. We recognized the value of Public Key Infrastructure (PKI) as central to securing our networks and conducting business over the Internet. This was thirteen years ago at a time when the projected cost was a significant barrier and technology was not yet sufficiently mature to achieve our goals. Nevertheless, we held to this objective and began a worthwhile journey.

During the past decade, the technologies have improved significantly and industry has provided solutions that have proven the value of conducting business over the Internet. With these changes, public sector PKI efforts have gained momentum. Examples include initiatives undertaken by the State of Iowa, the government of Canada and many Federal agencies, including the Department of Defense.

These positive activities indicated that the time was approaching where the U.S. government could safely conduct business with citizens and trading partners, while protecting individual privacy, intellectual property rights, and monetarily valuable information. Congress correctly decided that it was time to provide guidance to accelerate the exploitation of technology and concurrently to reduce obstacles to the use and acceptance of electronic signatures. As a result, the GPEA was signed into law in October 1998.

The path to electronic transactions is closely coupled to the maturation and affordability of the PKI. Through PKI digital signature, we will maintain and, in fact, improve the

integrity, authentication and non-repudiation that are necessary to assure trusted business interaction. The Department's initial focus has been to make PKI work for us internally in order to prove the technology, learn lessons through implementation, and make it simple for the users. We have been closely partnered with the Federal PKI efforts to leverage our efforts and to seek the best possible solution for the Department of Defense and those who conduct business with the government.

The path to achieving the objectives of GPEA has been a long one and the path has varied as the technical solutions have improved. The DoD issued its first comprehensive PKI policy in May 1999. We caveated it then with a promise to revisit the policy each year based upon lessons learned and developments in the private sector. In November 1999, we committed to using the Smart Card for our Common Access Card (CAC) to carry PKI tokens, which serve as identification certifications, for DoD employees. We partnered with the General Services Administration (GSA) to produce a government-shared solution. In August 2000, DoD updated our PKI policy to align PKI and CAC to the changing environment. During the intervening months, several industry consortia evaluated our policy and intended course of action and they confirmed that our path was compatible with the mainstream developments in industry.

The Department's activities have included consideration of how the private sector will be able to acquire and use PKI certificates for interaction with the federal government. The GSA created the Access Certificates for Electronic Services (ACES) contracts whereby the private sector, including private citizens, can get certificates. DoD assessed the initial ACES as providing relatively weak authentication. Consequently, DoD established Initial External Certification Authorities (IECAs) to issue certificates to our external partners at a security level that is adequate for the Department. Subsequently, the GSA improved ACES by adding business quality certificates, which have features comparable to the IECA. We are today exploring with the GSA the possibility of replacing the DoD IECA with the business quality certificates of ACES. This would provide a single approach for the private sector to authenticate themselves instead of the two approaches previously contemplated. This promises to be another positive step in our journey toward achieving the goals of GPEA.

The achievement of GPEA goals by DoD requires more than a PKI and external authorities to issue certificates to citizens and trading partners. It requires the DoD to enable the appropriate electronic applications to use and understand these new signature technologies. To that end, DoD published policy guidance on enabling applications. After a year of development and vetting, this guidance was issued on May 17, 2001. We are now working to enable mission applications. Again, the lessons learned in enabling mission applications will be used to enable the applications that interface externally, which are the applications that are necessary for GPEA compliance.

The Department is involved in a number of pilots and other initiative to validate our steps in the journey. These are necessary to prove that we can properly apply and scale these solutions. Examples of these activities include the following:

- DoD participated in the Federal Bridge Certificate Authority (FBCA) Pilot to prove interoperability between DoD, other federal departments, industry partners and the government of Canada. Now, the FBCA is working to establish trusted relationships with the State of Illinois. The education community is building an Education Bridge Certificate Authority that will eventually be cross certified with the Federal Bridge. DoD has provided the majority of resources to the FBCA.

- DoD is currently pursuing an initiative to utilize PKI in the export licensing process. This involves a coordinated effort to provide the export industry with the ability to submit license applications and supporting documentation electronically. This initiative will streamline the approval process and will involve the Departments of Defense, Commerce and State. It will include more than ten thousand businesses. To be successful, the initiative will require the interoperability of DoD issued certificates and ACES certificates, and the use of the FBCA. By early 2002, we will have real experience on the use of these pieces of the broader GPEA solution.

- The Department has made great strides over the past three years toward achieving the goal of a paper free end-to-end contracting process. To date, 81 percent of our contracting activity is paperless. Achieving the goal of a 100 percent paperless is dependent, in large part, on our ability to engage in trust commerce with our trading partners. Trusted commerce, in turn, is dependent on the implementation of a Public Key Infrastructure and the use of digital signature. Trusted commerce will eliminate the remaining security barriers to the electronic submission of claims for contract payments, the area that remains the most paperbound in the contracting process.

- The fiscal year 2001 National Defense Authorization Act directed the Department to move to the electronic submission and process of claims for contract payments, which we loosely call E-Invoicing. The target date for full compliance is October 2002 or one year before the GPEA target. As directed by Congress, the Defense Federal Acquisition Regulations will be modified to require all claims to be invoiced electronically. This covers our defense contractors and grant recipients. There are over 175,000 vendors registered in the DoD Central Contractor Registry (CCR) who will be required to interact with the Department electronically after they receive a contract or grant. Satisfaction of this requirement will move us much closer to the objectives of GPEA.

In summary, the path toward full compliance with GPEA is not only dependent upon improvements in technology and our ability to change our processes, but it is also the convergence of several key activities:

- A government-wide public key infrastructure with strong authentication using digital signature certificates that achieves a balance between security of and access to information;
- Enablement of applications and workstations;
- Issuance of acceptable certificates to the private sector; and
- Bridging to state governments and private sector communities of interest.

The Department of Defense will continue to pursue these activities and seek other ways to transform our processes and exploit information technology so that we can better serve the American public and improve mission performance.

We have also been asked to comment specifically on the work of the Under Secretary of Defense for Personnel and Readiness in implementing GPEA. Ms. Norma St. Claire is the Director for Information Management for Personnel and Readiness (P&R). She is here to answer any questions.

P&R has been very proactive in a number of areas for paperwork reduction and elimination. We all face the dueling challenges of accessibility versus security in the implementation of most of these capabilities. As the Department attempts to implement web-based capabilities, we must ensure that we do not increase the opportunity for fraud and that we ensure the security of personal information. In spite of these challenges, P&R has made significant progress in moving forward with a number of initiatives. They have a full Business Process Reengineering program that continues to identify opportunities for streamlining and elimination of paperwork.

First, the Common Access Card that I discussed earlier is a major initiative of the personnel community. The Common Access Card will replace the military identification card and will be used in conjunction with PKI applications to greatly expand our ability to accept digital signatures and access computer systems.

The Defense Personnel Records Imaging System (DPRIS) is another major initiative of the personnel community. This capability allows for automated access to records that have been digitized by the individual Services but in the past have only been available through manual intervention. This fully automates a process that has been administered through the use of paper forms and letters for queries, paper or microfiche copies for response, and paper correspondence in carrying out information requests and exchanges. We have worked with the Department of Veterans Affairs to ensure that they can use DPRIS to access records on line. DPRIS initial operating capability has been established between the Bureau of Naval Personnel and the Department of Veterans Affairs. We expect the Army to be on line by September 2001, with the Marine Corps following in 2002 and the Air Force in 2003. We are also evaluating the applicability of this system for use by the Department of Labor and the National Personnel Records Center.

P&R has also been working for over a year on a review of the approximately 400 forms that are used throughout the personnel management process. The first recommendations from the Forms Team focused on the 68 forms that are used in the Accessions Process. The team recommended that all but four of these forms could be either eliminated completely or fully automated with no paper copies. The recommendations were accepted in August of 2000 and we are now reviewing implementation time-lines. The Forms Team has moved on to the review of the remaining personnel management forms.

One of the most ambitious undertakings of P&R is the design and implementation of the Defense Integrated Military Human Resources System (DIMHRS). DIMHRS is an all Service, all Component, fully integrated personnel and pay management system. It will eliminate forms from all aspects of personnel and pay management. It will also eliminate duplicate data collection and provide web-based services to individual Service members as well as to personnel managers. DIMHRS will be implemented sequentially to each of the Services, with the Army coming on line first in CY 2003. Part of the review process mentioned above for elimination of forms is focused on how many of the forms can be eliminated before DIMHRS is available. All of them can be eliminated with DIMHRS. DIMHRS will be implemented using a COTS HR product (PeopleSoft) and will take advantage of all of the best business processes imbedded in the product.

All of the Services are fully participating in the design and development of DIMHRS. In the interim, each Service has developed capabilities that will help reduce and eliminate paper within the Service personnel communities. Four of these initiatives are Army Knowledge on Line, Sailor OnLine, Air Force Link and Marine OnLine. All of these implement paperless requests, self-service capabilities, and on-line access to information.

The Defense Civilian Personnel Data System (DCPDS) is substantially reducing the amount of paperwork generated in the administration of civilian employees of the Department of Defense. DCPDS is an automated processing and reporting personnel system currently supporting approximately 275,000 employee records in the Department. When fully deployed, DCPDS will support almost 800,000 records. The system places an automated human resources system at the desktop of supervisors and managers. Personnel actions, training documentation, position descriptions, and other personnel documents are created, forwarded, coordinated, processed, and finalized in an electronic medium, including the application of digital signatures. Supervisors and managers are able to access the system at any time from their desktop application to review employee information, initiate or check the status of actions, and to extract and review a variety of reports. DCPDS also includes an automated staffing program that supports the receipt and evaluation of electronic resumes. Through the DCPDS, civilian positions are established, classified, announced, and filled in a totally paperless environment.

The Under Secretary of Defense for Personnel and Readiness (USD(P&R)) also oversees training for the Department and has worked with the Services and the rest of the Department on a number of training initiatives. The Advanced Distributed Learning initiative significantly reduces paper and paperwork in several ways. It permits electronic transcripts, applications and payment for education and training. It also features electronic class materials, electronic books and digital laboratory experimentation all in lieu of traditional paper products. It incorporates paperless homework assignments, tests and other performance indicators.

Equally important, these on-line training initiatives have made training far more accessible to both military and civilian personnel and have made it possible for personnel to take courses that once required several weeks of travel to complete.

Also within the P&R family, the Defense Commissary Agency (DeCA) has implemented a number of processes that have resulted in operational efficiencies and the elimination of hardcopy requirements. Electronic Data Interchange (EDI) provides for electronic purchase orders, invoices and vendor pricing and advance shipping notices for the receiving process. We also have a web-based pricing system for small vendors and pay most of the vendors through electronic funds transfer (EFT). DeCA Intranet is used for publication of directives, forms and handbooks and provides an important interface to patrons.

In closing, I want to reiterate the Department's commitment to achieving the goals of the Government Paperwork Elimination Act (GPEA) by October 2003. We will continue to seek new ways to transform processes and exploit technology so that the Department can better serve the public and the nation.