

SCSCG 31 March, 2000 Report to Congress

Requirement (Public Law 106-65): *Not later than March 31, 2000, the Secretary of Defense shall submit to the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives a report containing a detailed discussion of the progress made by the senior coordinating group in carrying out its duties.*

The Department of Defense (Department) has undertaken an extensive effort to adopt Smart Card technology and fully exploit the potential that the technology offers as a tool for enhancing readiness and improving business processes. As part of this effort, the Department established the Smart Card Senior Coordinating Group (SCSCG). The SCSCG has been chartered to develop and implement Department-wide interoperability standards for the use of Smart Card technology, and to develop and implement a Department-wide plan to exploit the full potential that Smart Card technology offers. The key focus of the SCSCG is to champion a common Smart Card solution that is interoperable across the Department. The SCSCG will provide strategic direction and guidance to develop and implement Smart Card technology within the Department, and serve as the Department-wide clearing-house and advocate for smart card issues.

The SCSCG is addressing interoperability by integrating Smart Card requirements in close coordination with the Military Departments and Agencies, and the Public Key Infrastructure Program Management Office (PKI PMO), resulting in an integrated Department Smart Card effort. The outcome of this effort will be a fully interoperable, backwards compatible, and commercially derived solution capable of working with planned or legacy systems. This effort is targeting an initial implementation population of all active duty military personnel (to include the Selected Reserve), DoD civilian employees and eligible contractor personnel. The Deputy Secretary of Defense has directed that the Smart Card will be used as the Department's Uniformed Services identification card, provide physical access to buildings and controlled spaces, and supply logical access to the Department's computer networks and systems. The Department has taken a business-based approach to implementing Smart Card technology. This includes using the technology as an enabling tool for business process reengineering and performance improvement where key objectives, such as infrastructure reduction, mission enhancement, increased customer satisfaction, and improved quality of life, are met. This business-based approach will incorporate a migration strategy that takes advantage of the multiple technology capability of the Smart Card, to include the integrated circuit chip, magnetic stripe and barcode. With this approach, the SCSCG will ensure that best practices from both Government and private industry will be optimally employed.

The Department has already made significant progress this year in achieving these tasks. One of these tasks, resulting from direction of the Joint Requirements Oversight Council, is the development of a Joint Operational Requirements Document (ORD) for Smart Cards which is currently undergoing review and coordination prior to issuance later this year. Building on the Department's concerted efforts to develop and deploy a PKI across all of DoD, the Department has prepared the "Consideration of Smart Cards as the DoD PKI Authentication Device Carrier", a special report to Congress required by Section 374

DRAFT

SCSCG 31 March, 2000 Report to Congress

of Public Law 106-65 (National Defense Authorization Act for FY 2000). This comprehensive report evaluates, compares, and contrasts available technologies and “concludes that Smart Card technology offers the most feasible authentication mechanism to support the DoD PKI and to protect its critical information.”

The Department is committed to maximizing usage of Smart Card technology. Department-wide working groups which report to the SCSCG have been organized specifically to address critical issues, such as the allocation of computer memory and data storage of the Integrated Circuit Chip (ICC) along with the design and placement of information on the face (topology) of the Department’s Smart Card. The Department is maximizing use of existing assets and infrastructure to gain efficiencies, such as use of the Defense Enrollment Eligibility Reporting System and the Real-time Automated Personnel Identification System to issue and maintain smart cards, as they both currently support the Uniformed Services identification card. Additionally the Department will ensure that Smart Card and PKI specifications and capability are included in the planning of information technology investments.

Key stakeholders in these efforts include several Defense Agencies, such as the Defense Information Systems Agency, the National Security Agency, the Defense Logistics Agency, and the Defense Finance and Accounting Service, all of the Military Departments, and the Joint Staff. Other Government representatives contributing to this effort include the Veterans Administration along with the Department of Transportation. Many of these contributors have chartered smart card offices to closely coordinate these efforts.

Efforts are on going throughout the Military Departments. The Department of the Navy’s Smart Card Office, under the cognizance of the Department of the Navy’s Chief Information Officer, has implemented several Smart Card projects at both its shore and ship based facilities. Shore based facilities include the Naval training activities in the states of FL, IL, and VA, along with major operational stations in the states of CA, HI, and VA. Every recruit entering the Navy receives a Smart Card and uses several applications during recruit training. Applications include food service, medical, dental, stored value, training and mustering. In FY 1999, two carrier battlegroups, carrier airwings, and amphibious ready groups were outfitted with smart card technology. Efforts are underway this year to expend regional implementation, both ashore and afloat. The Department of the Army has partnered with the Defense Finance and Accounting Service, commercial banks and the Department of Treasury for stored value projects at several of its training facilities in the states of GA, KY, MO, OK, and SC. The Department of the Air Force has stored value smart cards projects at training facilities in CO and TX. The Air Force is also piloting a deployment readiness smart card application in FL and ID. The Army, Navy, Marine Corps and Air Force also have ongoing Joint projects in HI for food service and deployment readiness smart card applications. Several systems currently under development in the Department include smart card technology in the technical requirements.

DRAFT

SCSCG 31 March, 2000 Report to Congress

This significant Smart Card effort within the Department has received extensive support and cooperation from all involved. This close coordination will ensure that implementation of Smart Card technology by the Department will be successful, measured in terms of enhanced readiness and improved business processes.

DRAFT