May 9, 2005

MEMORANDUM FOR: Office of Management and Budget (OMB)

ATTN: Karen Evans, OMB

FROM: Federal Partnership for Interoperable Communications (FPIC)

SUBJECT: Response to Notice and Request for Comments on Draft Implementation Guidance for Homeland Security Presidential Directive 12 (HSPD-12)

Ms. Evans:

The purpose of this letter is to file comments in response to the OMB Notice and Request for Comments on the Draft Agency Implementation Guidance for HSPD-12, dated April 8, 2005. This agency implementation guidance provides specific instructions to agency heads on how to implement the Directive and the Federal Information Processing Standard (FIPS) 201. The Federal Partnership for Interoperable Communications (FPIC)[1] supports this transition and agrees with the implementation of a common identity management solution across the Federal Government. However, the FPIC proposes that OMB grant a waiver of the HSPD-12 requirement for common identification credentials when requesting logical access to federally controlled information systems. This waiver is critically important to federal owners, operators, and users of *tactical wireless systems*, a category that includes land mobile radio (LMR) systems, maritime mobile radio (MMR) systems, high frequency (HF) emergency response radio systems, technical investigative systems, wireless sensor network, and remote telemetry systems. Implementation of HSPD-12 requirements would greatly impede agencies' ability to carry out their legal responsibilities and authorities.

The Nation's public safety communications systems are key components in ensuring the protection of the homeland. These systems support first responders, law enforcement officers, fire and emergency medical responders, investigators, and homeland defense forces. The federal public safety communications community includes more than 100,000 officials in more than 20 departments and agencies. The communications infrastructure supporting these officials includes mobile radio service networks to support public safety operations; technical investigative systems to support law enforcement operations; HF radio networks to support emergency response and tactical missions; and wireless sensor networks and remote telemetry systems, such as those along U.S. borders. The Federal Government has invested hundreds of millions of dollars over the past decades to build, operate, and maintain these networks—and a substantial portion of this investment has been focused on deploying secure and reliable systems.

[1] Wireless communications solutions, and interoperability issues in particular, have been a top priority for the Federal Government in near-term operational planning and budgeting for more than 10 years. Specifically, the Federal Law Enforcement Wireless Users Group (FLEWUG) was established in 1994 to help raise the level of awareness across the federal law enforcement community regarding key issues associated with wireless communications such as security and interoperability. FLEWUG would eventually become the *Federal Partnership for Interoperable Communications* (FPIC), which now stands as an active and important technical and operational advisor that helps implement priorities raised by the entire federal wireless communications community and takes an active role in federal interoperability efforts.

The FPIC members are concerned that implementing HSPD-12 on tactical wireless systems will jeopardize the ability of the Nation's public safety communications infrastructure to support critical law enforcement and homeland security mission objectives, including emergency preparedness and response. The FPIC members have three concerns with this implementation plan:

- The first and most important concern is that a rapid cutover to FIPS-201 compliant identification processes could result in service disruptions and performance degradation for public safety officers and agents in the field. To accomplish this implementation, more than 100,000 subscriber units and tens of thousands of other wireless devices must be taken out of service and upgraded—and this must be done in coordination with significant infrastructure deployments to support credential management. This entire operation must be performed on fully operational systems that support real-time public safety tactical operations. Upgrades of this size and scope cannot be allowed to threaten the safety of users in the field (including state and local partners), endanger the public welfare, or compromise national security. The FPIC does not believe that this implementation can be accomplished safely within the proposed timeline.

- The second concern is the high cost of this transition for the federal public safety community. As one example, the Department of Homeland Security is in the process of converting its legacy LMR infrastructure and subscriber equipment to the Advanced Encryption Standard (AES) in order to meet new FIPS compliant encryption requirements. This transition, which affects tactical wireless systems covered by HSPD-12, is projected to cost in excess of $150 million over the 2-year transition period. Accomplishing a separate FIPS-201 implementation of this magnitude within OMB's proposed timeline will have an immediate and direct impact on organizations' abilities to meet critical mission requirements.

- The third concern is the availability of FIPS-201 compliant solutions that can be implemented on tactical wireless systems. Historically, tactical wireless systems have not been categorized as information technology (IT) assets by federal agencies. However, in recent years, manufacturers of these systems have begun to implement industry-standard network protocols (e.g., TCP/IP) and computer-based control mechanisms—but these systems are still largely composed of special-purpose electronic devices such as portable radios, radio repeaters, and dispatch consoles. Even though these systems are now largely treated as IT assets by federal agencies, there are virtually no commercially-available solutions that will enable agencies' diverse portfolios of tactical wireless systems to become compliant with HSPD-12 requirements.

With these issues in mind, the FPIC proposes that OMB grant waivers from HSPD-12 authentication requirements for specific federal tactical wireless systems, where requested by federal departments and agencies. The category "tactical wireless systems" includes (but is not limited to) the following types of systems and technologies:

- LMR systems
- MMR systems
- HF emergency response radio systems
- Technical investigative systems

- Wireless sensor networks
- Remote video surveillance systems
- Remote telemetry systems.

The FPIC recommends that OMB encourage agencies to adopt acquisition policies that allow all future tactical wireless system acquisitions to be HSPD-12 compliant, when this compliance is both technically and operationally feasible. In some cases, such as with wireless covert surveillance systems, HSPD-12 compliance will never be operationally feasible without compromising officer safety. In other cases, such as with mobile radio systems, future generations of equipment will likely be equipped for advanced authentication and identity management functions—and these systems could be retrofitted with FIPS-201 compliant solutions in the coming years. OMB should allow for a smooth transition that allows owners, operators, and users to use existing tactical wireless equipment through a reasonable lifecycle while continuing to upgrade tactical wireless systems and equipment to be compliant with HSPD-12 where feasible.

Response to this request can be directed to the FPIC chair, Jim Downes, at james.downes@dhs.gov or (703) 279-2012

Respectfully submitted,

James E. Downes,
Chair, Federal Partnership for
Interoperable Communications (FPIC)