"Taken from Senate Report 107-156
MAKING SUPPLEMENTAL APPROPRIATIONS FOR FURTHER RECOVERY FROM AND RESPONSE TO TERRORIST ATTACKS ON THE UNITED STATES FOR THE FISCAL YEAR ENDING SEPTEMBER 30, 2002, AND FOR OTHER PURPOSES…"

DEPARTMENT OF COMMERCE

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

SCIENTIFIC AND TECHNICAL RESEARCH AND SERVICES

2002 appropriation to date	$680,751,000
2002 supplemental estimate	4,000,000
Committee recommendation	84,600,000

The Committee recommends a total appropriation of $84,600,000 for the National Institute of Standards and Technology (NIST). The recommendation is $80,600,000 above the supplemental budget request. Of this amount, $22,000,000 is for standards development for chemical/biological/nuclear/radioactive explosive threat detection equipment and biomedical recognition equipment to support homeland security activities. This amount will also strengthen security and surveillance at the NIST neutron reactor.

The Committee recommendation includes $16,600,000 is for equipping the Advanced Measurement Laboratory (AML). The funds will strengthen a broad range of homeland security activities by enabling NIST to provide the most demanding measurements and standards in support of advanced homeland security technologies. Advanced measurement and research equipment is needed to ensure that the AML will become a critical tool for NIST's development of the most advanced measurements and standards to support homeland security.

In addition, $6,000,000 is provided for standards, technology and practices for buildings and emergency responders to develop and implement cost-effective safety and security of buildings, including emergency response.

Senate Report 107-156 continued…

Specifically, the recommended funding will be used to initiate a portion of critical needs in three technical areas: (1) Improving fire resistance test methods for connections and components in steel structures; (2) Developing performance measures for equipment used by first responders, including demonstration of enhancements to re-create simulation tool for fire and smoke movement in tall buildings; and (3) Developing guidelines and advanced technologies to reduce the vulnerability of civilian buildings to chemical, biological and radiological attacks.

Adequate and reliable wireless communications is an issue affecting the state and local public safety community. The NIST has been involved in projects working to resolve this issue for the past 3 years. During the past 3 years, NIST's Office of Law Enforcement Standards (OLES) has concentrated most of its technical efforts toward a major program of the Department of Justice, National Institute of Justice (NIJ) called the Advanced Generation of Interoperability for Law Enforcement (AGILE).

OLES recently completed the AGILE Strategic Plan for developing information technology information-sharing standards, as well as all of its accompanying documents. All background documents for a Wireless Standards Strategic Plan were also developed. The Strategic Plan associated with wireless telecommunications interoperability is being finalized by identifying the proper public safety practitioners to represent wireless users. This finished the preparation phase for information technology standards development, and allowed OLES to work with public safety information technology practitioners to develop the standards. OLES also performed a formal technical evaluation of an audio gateway device. Labeled a `cross-banding technology,' the equipment allows the interoperation of dissimilar wireless telecommunication systems, for example between very high frequency radios and ultra-high frequency radios.

To further expand its efforts in interoperable communication standards for first responders, the Committee recommendation includes $5,000,000 to be transferred from the Community Oriented Policy Services, Interoperable Communications Technology program to NIST's Office of Law Enforcement Standards. The recommended funding will provide coordination and management in the development of the following: (1) Public safety communications standards geared toward solving public safety interoperability and information sharing problems by developing and adopting NIJ standards for voice, data, image, and video information transfers; (2) examinations of requirements and development of standards for interoperable communications interfaces with protective equipment ensembles and respiratory protective equipment for emergency first responders, in particular for firefighters and for bomb suits; (3) Integrated approaches for automated integration of communications infrastructure systems and development of supporting standards, methods, and tools to improve interoperability of these integrated systems; and (4) sensing, perception and modeling

Senate Report 107-156 continued…

technologies to improve the situational awareness of first responders and help locate victims in adverse conditions. The Committee expects NIST to finalize these standards within 12 months of enactment of this Act.

The Committee recommendation includes $40,000,000 for a Cyber-Security Initiative. Critical Federal information and systems are at grave risk to exploitation due to inadequate security. Federal officials responsible for running large Federal programs are making important information technology security judgments on the basis of incomplete, irrelevant, and inadequate information. Huge investments are being made in building new Federal systems that will be vulnerable from `day one.' Security critical information technology products that protect critical information are configured today so they are easily exploitable. Federal agencies are providing inconsistent protection of sensitive information and critical systems due to a lack of definitive, up-to-date, and comprehensive guidance.

To address this problem, the Committee recommendation includes $30,000,000 for NIST to develop the following: (1) unified Federal guidelines and procedures for conducting system security certification, and a complimentary program to validate the technical security competence of organizations that perform these complex systems security reviews; (2) an Information System Security Architectural Assistance capability that agencies can draw upon to help review and improve proposed system security architectures; (3) security benchmarks for widely-used information technology security products and complimentary automated tools for system administrators to measure compliance; and (4) security guidelines in gap areas and overhaul of outdated security guidelines to secure sensitive Federal information technology assets.

The security of information technology system components, key security technologies, and resulting composed systems, cannot be scientifically measured leaving the nation with inadequate information regarding the state of our cyber defenses. Currently, there is no comprehensive and scientifically rigorous methodology to test the effectiveness of systems. For example, there are no standards for measuring the security of intrusion detection systems or embedded systems such as those in cellular telephones and electronic organizers. Security architectures and protocols for embedded systems are largely unexplored, leaving these systems vulnerable to numerous forms of attack. Inadequate technical means exist for organizations to enforce strong policies on access to information on our systems. Without means to measure the quality of security in all these types of systems, organizations have little knowledge of the state of their security and have difficulty justifying security resource expenditures based upon expected improvements. Security resources may be misapplied while serious vulnerabilities remain unaddressed.

Senate Report 107-156 continued…

To address these concerns, the Committee recommendation includes $6,000,000 for NIST to: (1) develop advanced methods to express security requirements in ways that support secure composability and measurability to enable rapid testing with more comprehensive qualitative coverage; (2) design and architect better metrics, reference data, and ultimately more testable security architectures; (3) build and operate an intrusion detection test bed in order to develop a rigorous methodology and test regime for intrusion detection systems to improve the security capabilities of such important system security defenses; (4) develop a coordinated Embedded Systems Security Architecture program to identify embedded system vulnerabilities, develop corrective prototype/proof-of-concept security systems and develop corresponding standards and conformance tests; and (5) develop an advanced access control and management architecture to enforce strong access control policies.

In addition, the Committee recommendation includes $4,000,000 for a wireless security initiative. Minimal security exists to protect the ever-growing array of mobile and wireless systems now being deployed. Today's security solutions operate poorly within the constraints of mobile deployment, making wireless networks far more vulnerable than wired networks. Wireless security technology today cannot begin to adequately protect the government, corporate, and personal information that individuals wish to access with wireless mobility. Not only are the communications protocols flawed, but controls on access, availability and confidentiality of information on lightweight, mobile devices is inadequate. To address this problem, the Committee directs NIST to develop technologies to promote, enable, and enforce security on mobile devices, develop secure prototypes, and develop use of mobile code to secure wireless systems.

The Committee supports NIST's continued collaboration with the Department of Defense and other appropriate agencies in its effort in biometrics and cyber security.