BRIEFING PAPERS® SECOND SERIES

WEST®

PRACTICAL TIGHT-KNIT BRIEFINGS INCLUDING ACTION GUIDELINES ON GOVERNMENT CONTRACT TOPICS

INFORMATION SECURITY FOR FEDERAL AGENCIES & CONTRACTORS

By David Z. Bodenheimer and Jonathan M. Baker

In the Information Age, both the public and private sectors run upon continuous flows of real-time data interconnected by a vast system of information technology infrastructure. The U.S. information and communications sector alone contributes over $1 trillion per year to the nation's economy.[1] President Obama has aptly characterized "America's digital infrastructure" as "the backbone that underpins a prosperous economy and a strong military and an open and efficient government."[2]

In the information realm, no one is a bigger player than the Federal Government and its contractors. As a result, both the public and private sectors bear substantial roles and responsibilities in protecting the federal IT infrastructure and the treasure troves of highly sensitive information flowing through it.

This Briefing Paper explores three major aspects of information security for federal agencies and contractors. First, federal information security represents a high-stakes enterprise because security breaches of federal databanks and IT systems pose potentially catastrophic risks and attract the world's most dangerous hackers. Second, an expanding set of statutory, regulatory, and administrative rules governs federal information security, placing a greater premium on compliance and exposing agencies and contractors with weak cybersecurity to escalating risks and tougher congressional

IN BRIEF

David Z. Bodenheimer is a partner in the Washington, D.C. office of Crowell & Moring LLP, where he heads the Homeland Security Practice and specializes in Government contracts, False Claims Act, privacy, and cybersecurity litigation, investigations, and counseling. Jonathan M. Baker is an associate in the firm's Washington, D.C. office, where he practices in the Government Contracts group.

  4-115-332-6

and Executive Branch scrutiny. Third, effective cybersecurity depends upon a commitment to a sound information security program built upon procedures, controls, continuous monitoring, training, and enforcement, as described below.

Why The Stakes Are So High For Cybersecurity In The Federal Sector

Three key factors explain why the stakes are so high for cybersecurity in the federal sector—and why effective security is so hard. First, the Federal Government holds, uses, and moves more information than any other entity in the world, thus making it a prime target for hackers everywhere. Second, federal cybersecurity hinges upon information sharing both within Government (federal, state, and local) and between the public and private sectors, thus creating substantial logistical and organizational challenges that strain the perimeters of cyber defenses guarding such information. Third, the cyber threat has dramatically escalated in magnitude and frequency, jeopardizing national security, economic power, and personal privacy.

The gravity of these risks to cybersecurity has been emphasized at the highest levels of Government—and in the starkest terms. As President Obama stated, "[t]he status quo is no longer acceptable."[3] Members of Congress from both parties have described the threat as a "catastrophe" in the making.[4] In sizing up the threat, Defense Secretary Leon Panetta compared it to a digital "Pearl Harbor":[5]

> We have to continue to focus on the threat of cyber attacks. We're now in a very different world, where we could face a cyber attack that could be the equivalent of Pearl Harbor. Someone using cyber can take down our power grid, our financial systems in this country, our government systems [and] our banking systems. They could virtually paralyze this country.

Given such factors, federal agencies and contractors can expect much greater scrutiny in the information security realm as both the President and Congress apply greater pressure to enforce existing security rules, apply stricter oversight, and implement tougher cybersecurity standards.

■ World's Largest Information Data Banks

In the global information economy, nobody handles more data than the U.S federal sector. In past reports, the Office of Management and Budget has underscored the sheer magnitude of the Federal Government's job in the information business:[6]

> The Federal government is the largest single producer, collector, consumer, and disseminator of information in the United States and perhaps the world.

Why do hackers worldwide seek to rob these federal data banks? To paraphrase bank robber Willie Sutton, "because that's where the information is." As one congressman put it, "our extensive digital networks and information systems provide a rich target for thieves and rogue nations."[7] This treasure trove of federal information includes everything from national security secrets and critical infrastructure data to private sector trade secrets and highly sensitive personal information and healthcare data.

With this status as the world's 800-pound information gorilla comes enormous responsibility for protecting federal information from hostile nations,

WEST®

BRIEFING PAPERS

BRIEFING PAPERS® (ISSN 0007-0025) is published monthly except January (two issues) and copyrighted © 2012 ■ Valerie L. Gross, Editor ■ Periodicals postage paid at St. Paul, MN ■ Published by Thomson Reuters / 610 Opperman Drive, P.O. Box 64526 / St. Paul, MN 55164-0526 ■ http://www.west.thomson.com ■ Customer Service: (800) 328-4880 ■ Postmaster: Send address changes to Briefing Papers / PO Box 64526 / St. Paul, MN 55164-0526

terrorists, organized crime, and even casual hackers bent upon breaking into federal information systems and stealing high-value information. Given the magnitude and value of information in the hands of the Federal Government and its contractors, nowhere in the world is the need for information security greater than in the federal sector.

■ The Mandate For Information Sharing

Just as the homeland security mission hinges upon information sharing ("connecting the dots"), effective cybersecurity requires a coordinated defense based upon real-time, two-way information sharing both within the Federal Government itself and between the public and private sectors. The President, Congress, and industry have consistently recognized the need for such information sharing for effective cybersecurity. For example, the President's Cyberspace Policy Review explained:[8]

> Information is key to preventing, detecting, and responding to cyber incidents. Network hardware and software providers, network operators, data owners, security service providers, and in some cases, law enforcement or intelligence organizations may each have information that can contribute to the detection and understanding of sophisticated intrusions or attacks. A full understanding and effective response may only be possible by bringing information from those various sources together for the benefit of all.

Legislation introduced in Congress would "facilitate the exchange of cyber information and intelligence to accelerate cyber threat identification and remedies."[9] Similarly, industry has consistently advocated the need for expanded information sharing to bolster cybersecurity.[10]

While information sharing is an essential component of cybersecurity, such sharing comes with its own security risks, as illustrated by the WikiLeaks breach where the "lack of management and technical controls…allowed a Private in the Army allegedly to steal some 260,000 classified State Department cables and 90,000 intelligence reports."[11] As a result, both agencies and contractors must focus not only upon effective—but also secure—information sharing by establishing management and technical controls to prevent necessary information sharing from becoming a major security gap in cyber defenses.

■ Escalating Cyber Threats To The Federal Sector

Given the reams of high-value information residing in the federal data banks, federal agencies and contractors have been under continual siege by escalating cyber attacks, as described in a Center for Strategic and International Studies report:[12]

> The damage from cyber attack is real. In 2007, the Departments of Defense, State, Homeland Security, and Commerce; NASA; and National Defense University all suffered major intrusions by unknown foreign entities. The unclassified e-mail of the Secretary of Defense was hacked, and DOD officials told us that the department's computers are probed hundreds of thousands of times each day. A senior official at the Department of State told us the department lost "terabytes" of information. Homeland Security suffered break-ins in several of its divisions, including the Transportation Security Agency. The Department of Commerce was forced to take the Bureau of Industry and Security off-line for several months, and NASA has had to impose e-mail restrictions before shuttle launches and allegedly has seen designs for new launchers compromised. Recently, the White House itself had to deal with unidentifiable intrusions in its networks.

Since this 2008 report, the attacks on federal agencies have only intensified in frequency and gravity. In 2009, "the Pentagon reported more than 360 million attempts to break into its networks."[13] By 2010, the probes or attacks on federal information networks numbered in the billions.[14] In 2011, a congressional oversight committee reported that "the number of cyber incidents affecting federal agencies shot up 39 percent in 2010."[15]

(1) *National security threats.* As a key finding in its 2008 report, the CSIS Commission on Cybersecurity warned that "America's failure to protect cyberspace is one of the most urgent national security problems."[16] In January 2009, former Director of National Intelligence Mike McConnell "equated 'cyber weapons' with weapons of mass destruction when he expressed concern about terrorists' use of technology to degrade the nation's infrastructure."[17] Incidents underscoring the gravity and reach of this threat include:

(a) *Malware attack.* "In one of the most serious cyber incidents to date against our military networks, several thousand computers were infected [in 2008] by malicious software—malware."[18]

(b) *Presidential helicopter.* "The U.S. Navy is investigating how an unauthorized user in Iran gained online access to blueprints and other information about a helicopter in President Obama's fleet."[19]

(c) *Lost military secrets.* "[T]he State and Defense Departments have lost more than six or seven terabytes of information to digital espionage—an amount equal to approximately one-sixth of the information contained in the entire Library of Congress."[20]

(2) *Economic damage.* Cyber attacks also steal critical technology, military know-how, and industry trade secrets, sapping the economic power that fuels U.S. military might and national commerce. As stated in the President's Cyberspace Policy Review, "[o]ur digital infrastructure has already suffered intrusions that have allowed criminals to steal hundreds of millions of dollars and nation-states and other entities to steal intellectual property and sensitive military information."[21] For such security breaches, the economic stakes are enormous:

(a) *$1 trillion thefts.* "According to a 2009 report from McAfee, the 2008 overall losses from data theft and breaches from cybercrime may have cost businesses as much as $1 trillion globally in lost intellectual property and expenditures for repairing the damage [in 2008]. Respondents estimated that they lost data worth a total of $4.6 billion and spent about $600 million cleaning up after breaches."[22]

(b) *Terabyte data losses.* "As an example of the scale of the threat, one American company had 38 terabytes of sensitive data and intellectual property exfiltrated from its computers—equivalent to nearly double the amount of text contained in the Library of Congress."[23]

(c) *Digital 9/11 impact.* "According to the National Journal, Mike McConnell, the former Director of National Intelligence, told President Bush in May 2007 that if the 9/11 attackers had chosen computers instead of airplanes as their weapons and had waged a massive assault on a United States bank, the economic consequences would have been 'an order of magnitude greater' than those caused by the physical attack on the World Trade Center."[24]

(d) *$7 million impact per breach.* "The average cost of a data breach hit $7.2 million [in 2010] and cost companies $214 per compromised data record, according to the Ponemon Institute. And that's just for a data breach. If a company's intellectual property is stolen, it could decimate an organization."[25]

(3) *Personal impact.* Security breaches also strike with the unpleasant personal force of a punch in the gut, violating privacy and stealing identities: "Almost every day, new data breach incidents lead to identity theft, lost revenue, and decreased consumer confidence in the way their personal information is handled in the marketplace."[26] Security breaches have affected both the public and private sectors, compromising over a half billion records containing personal information: "According to the Privacy Rights Clearinghouse, over 2,500 data breaches implicating nearly 600 million records have been made public since 2005," with over 99 million records of personal information being exposed in April 2011 alone.[27] Federal agencies, employees, military personnel, and contractors have been hit particularly hard:

(a) *4.9 Million TRICARE members.* "The Defense Department has been hit by a $4.9 billion class action lawsuit filed on behalf of four military family members and the 4.9 million Tricare beneficiaries whose personal information was contained on tapes stolen from a car in San Antonio in September [2011]."[28]

(b) *26 million veterans.* "In May 2006, the Department of Veterans Affairs lost an unsecured laptop computer hard drive containing the health records and other sensitive personal information of approximately 26.5 million veterans and their spouses."[29]

(c) *Navy CIO victimized.* "The personal identifiable information of the Navy chief information officer has been compromised,

again. And, it isn't just the second or third or fourth or even fifth time [the CIO's] PII has been exposed, but the sixth instance."[30]

(d) *Defense Secretary hacked.* "The Secretary of Defense's unclassified e-mail was hacked."[31]

In summary, cyber assaults on the U.S. threaten its military might and economic power and the personal well-being of its citizens. And the situation will get much worse—perhaps seriously so—if treated as a lingering inconvenience rather than as a looming material threat. Accordingly, both agencies and contractors can expect tougher enforcement of the information security laws and standards discussed below.

What Cybersecurity Rules Apply In The Federal Sector

No single statute or regulation defines the totality of information security requirements governing the federal arena. Instead, variations in requirements may arise due to a host of factors, including the classification of the information (classified versus unclassified), the nature of the Government network (military versus civilian agencies), or the type of the data (personal information, healthcare data, etc.). The summary of federal information security standards below is not exhaustive but is intended to capture the primary statutes, regulations, and standards governing federal agencies and contractors. Furthermore, this summary will focus upon unclassified information, given that separate statutory and regulatory regimes cover classified national security information for military and intelligence agencies.

■ Statutory Requirements

The Federal Information Security Management Act establishes broad mandates for securing federal information systems and data.[32] As a statutory purpose, Congress in FISMA sought to "provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets."[33]

Except for "national security systems," the statute designates the OMB Director as having the authority to "oversee agency information security policies and practices," including overseeing implementation of security policies and standards, requiring agencies to "provide information security protections," coordinating security standards with the National Institute of Standards and Technology, overseeing agency compliance with FISMA, conducting annual reviews, and reporting to Congress.[34] For "national security systems," the Secretary of the Department of Defense and the Director of the Central Intelligence Agency have responsibility for their respective information systems.[35]

For federal agencies, FISMA places responsibility specifically upon the "head of each agency" for meeting information security requirements.[36] These responsibilities include establishing "information security protections," implementing "an agencywide information security program," and providing annual reports to Congress and the OMB Director.[37] In addition, each agency must subject its information security program and practices to an annual "independent evaluation" conducted by the agency's Inspector General or by an "independent external auditor" and report these audit results to the OMB Director.[38]

Under certain circumstances, FISMA may also apply to federal contractors. In particular, the statute states:[39]

> The head of each agency shall—
>
> (1) be responsible for—
>
> (A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—
>
> (i) information collected or maintained by or *on behalf of the agency*; and
>
> (ii) information systems used or operated by an agency or *by a contractor* of an agency or other organization *on behalf of an agency*[.]

The purpose of this subsection is to prevent agencies from avoiding their FISMA obligations simply by outsourcing federal data collection or federal information system operation or use to contractors.

In addition to FISMA, the Privacy Act may have significant implications for federal information

security.[40] This statute generally bars federal agencies from disclosing records containing an individual's personal data (e.g., name or other identifying information linked to "education, financial transactions, medical history, and criminal or employment history") unless that individual consents to such disclosure.[41] While this statute does not define specific requirements for information security, it may impose serious sanctions for unauthorized disclosure of personal information, including criminal penalties, civil remedies, and administrative sanctions.[42] For example, a DOD security breach potentially exposing medical data for 4.9 million TRICARE participants has triggered a $4.9 billion class action based upon the Privacy Act's minimum civil penalties of $1,000 per unauthorized disclosure.[43]

The Privacy Act may also apply to Government contractors that operate an agency's system of records to accomplish an agency function.[44] The Privacy Act's civil remedies do not apply to Government contractors.[45] However, such contractors may be subject to criminal sanctions for Privacy Act violations.[46] In addition, an improper disclosure of Privacy Act data may expose a contractor to agency contractual claims for breach, as well as to congressional inquiries suggesting that the contractor be banned from receiving further federal contracts due to data security breaches.[47]

■ Regulatory Requirements

The Federal Acquisition Regulation contains several high-level requirements relating to information security and privacy. In the acquisition planning phase, the regulations require agencies to prescribe procedures:[48]

> Ensuring that agency planners on information technology acquisitions comply with the information technology security requirements in the Federal Information Security Management Act (44 U.S.C. 3544), OMB's implementing policies including Appendix III of OMB Circular A-130, and guidance and standards from the Department of Commerce's National Institute of Standards and Technology.

Similarly, the FAR specifies "security policies and requirements" to be incorporated into acquisitions for IT:[49]

> In acquiring information technology, agencies shall include the appropriate information technology and security policies and requirements, including use of common security configurations available from the National Institute of Standards and Technology's Web site at *http://checklists.nist.gov*.

The regulations also mandate security and safeguards to protect data subject to the Privacy Act, including a program for Government inspection of the contractor's safeguards against new threats and hazards.[50]

In revising the FAR to implement FISMA, a Federal Acquisition Circular specifically addressed information security requirements applicable to Government contractors:[51]

> Section 301 of FISMA ([44 U.S.C.A. §] 3544) requires that contractors be held accountable to the same security standards as Government employees when collecting or maintaining information or using or operating information systems on behalf of an agency.… The law requires that contractors and Federal employees be subjected to the same requirements in accessing Federal IT systems and data.

The FAR itself does not establish detailed rules on information security, but instead recognizes that "[a]gencies will customize IT security policies and implementations to meet mission needs as they adapt to a dynamic IT security environment."[52] For example, the General Services Administration has developed detailed requirements for contractors that connect to GSA information systems, operate information systems for the GSA, and/or have access to GSA information.[53] Key GSA requirements for information security include the following:

(1) *Overall responsibility.* The contractor bears responsibility for information security for (1) all systems connected to a GSA network or operated by the contractor for the GSA and (2) physical or electronic access to the GSA's information.[54]

(2) *IT security plan.* The contractor must prepare and submit an IT security plan describing processes and procedures compliant with FISMA and the GSA security guide.[55]

(3) *Continuous monitoring.* The contractor must develop a continuous monitoring plan addressing configuration management, ongoing security control assessments, and reports to GSA officials.[56]

(4) *Security authorization.* The contractor has six months to submit proof of IT security authorization, including a final security plan, risk assessment, security test and evaluation, disaster recovery plan, and continuity of operations plan.[57]

(5) *Annual verification.* The contractor must submit annual verification that the IT security plan remains valid.[58]

(6) *Training.* The contractor must ensure employees working on the contract receive annual IT security training consistent with FISMA, OMB, and NIST standards.[59]

(7) *GSA access.* The contractor must afford the GSA access to the contractor's and subcontractor's facilities, installations, operations, documentation, databases, IT systems and devices, and personnel used in performance of the contract so that the GSA can conduct inspections, evaluations, investigations, and/or audits of IT security.[60]

The DOD and its military departments generally operate under a separate statutory and regulatory regime due to their responsibility for "national security systems."[61] The Defense FAR Supplement refers to this statutory authority and incorporates specific DOD directives governing information security.[62] In general, DOD departments and contractors implement information security pursuant to the DOD Information Assurance Certification and Accreditation Process directives and instructions.[63]

Other agencies have also issued specific regulations governing information security for Government contractors. Examples include the Departments of Homeland Security,[64] Health and Human Services,[65] Energy,[66] and Veterans Affairs.[67] As a general rule, these regulations expressly refer to the authority established by FISMA and incorporate requirements and standards defined by the OMB and NIST.

■ Security Policies & Standards

The FISMA and implementing regulatory requirements have been fleshed out in both OMB guidance and NIST standards. At first blush, these Government "standards" might appear to be mere guidance, rather than real mandates. However, FISMA specifically requires agencies to "ensure compliance with…policies and procedures as may be prescribed by the [OMB] Director, and information security standards promulgated under [40 U.S.C.A. §] 11331."[68] Similarly, these statutory provisions referenced in FISMA use mandatory language to describe information security standards issued by NIST: "Information security standards described under subparagraph (B) [NIST 'minimum information security requirements'] shall be *compulsory and binding*."[69]

In the regulatory provisions governing information security, as noted above, the FAR expressly requires agency procedures ensuring compliance not only with FISMA, but also with the "OMB's implementing policies including Appendix III of OMB Circular A-130, and guidance and standards from the Department of Commerce's National Institute of Standards and Technology."[70] In implementing these information security standards, the FAC stated the objective of "[r]equiring adherence to Federal Information Processing Standards" issued by NIST.[71]

In 2010, the OMB assigned the DHS the "primary responsibility within the executive branch for the operational aspects of Federal agency cybersecurity with respect to the Federal information systems that fall within FISMA under 44 U.S.C. § 3543."[72] Pursuant to this authority, the DHS has emphasized greater focus upon continuous monitoring as an essential component of federal information security.[73] In addition, the DHS has underscored the applicability of FISMA requirements to "contractors, grantees, State and Local Governments, industry partners, providers of software subscription services, etc."[74] Although not an exhaustive list, the DHS identified five categories of contractors most likely to be subject to FISMA requirements:[75]

(1) *Service providers*—e.g., services relating to outsourcing of system or network operations, telecommunications services, or other managed services, like subscriptions to software services.

(2) *Contractor support*—e.g., on- or off-site contractor technical or other support staff.

(3) *Government-owned, contractor-operated (GOCO) facilities*—e.g., operations where contractors operate Government-owned facilities on behalf of federal agencies.

(4) *Laboratories and research facilities*—e.g., operations involving contractors working at federal laboratories and research facilities.

(5) *Management and operating contracts*—e.g., contracts for the operation, maintenance, or support of Government-owned or –controlled research, development, special production, or testing establishments.

The guidance from the OMB, the DHS, and NIST reflect the greater scrutiny that both agencies and contractors can expect from both Congress and the Executive Branch regarding information security. These standards are discussed in greater detail below in the section of this BRIEFING PAPER addressing the key elements of an effective information security program.

What Are The Key Elements Of A Sound Information Security Program

The OMB and NIST standards alone span thousands of pages. However, the major elements of an effective information security program may be broken down into four general steps: (1) establishing security objectives, (2) identifying security needs, (3) implementing the security program, and (4) ensuring compliance.

Establishing Security Objectives

The core objectives of an information security program are straightforward and largely established by statute and regulation. FISMA defines "information security" to mean "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction" to maintain the "integrity," "confidentiality," and "availability" of such information.[76] Guidelines for defining the potential impact (low, moderate, or high) for security breaches resulting in a loss of confidentiality, integrity, or availability appear in the Federal Information Processing Standards Publications.[77] These key objectives—integrity, confidentiality, and availability of information—are defined in both FISMA and the implementing regulations. A security program may sweep in other objectives as well, but these must be included at a minimum.

(a) *Integrity*. Integrity essentially means the information is real and not changed without authorization. It requires "guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity."[78]

(b) *Confidentiality*. Confidentiality encompasses both access and disclosure restrictions. It requires "preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information."[79]

(c) *Availability*. Availability covers the spectrum from the mundane (information appears on the computer screen when requested) to the catastrophic (information is recovered after a disaster). It requires "ensuring timely and reliable access to and use of information."[80]

Identifying Security Needs

Prior to developing an information security program, the security requirements, risks, cost-effectiveness, and life-cycle impact all need to be addressed. These factors will then define the size and shape of the security program to be implemented.

■ Requirements Identification

Identifying the applicable requirements represents an initial step in determining the contours of the information security program. FISMA states that the "policies, procedures, and control techniques" must "address all applicable requirements."[81] Such requirements include not only FISMA itself ("this subchapter"), but "any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President."[82] While this statutory provision does not identify specific standards, it would appear to

include both OMB Circular A-130 and the NIST standards.[83]

■ Risk Assessment

Information security is not one-size-fits-all, but instead must be tailored to the particular risks associated with the information, the IT systems, and the organization's mission and needs. The rules contemplate an initial risk assessment as well as periodic reassessments.

(1) *Initial risk assessment.* A risk assessment ("assessing the risk and magnitude of the harm that could result") is fundamental to determining the scope and depth of protection needed for information security.[84] Indeed, the policies and procedures "are based on the risk assessments."[85] Similarly, the FAR implementation recognizes that the "information security protections" must be "commensurate with security risks."[86]

(2) *Periodic risk assessments.* Just as computers change and hackers become more sophisticated, FISMA contemplates that the risk assessment will be updated with "periodic assessments of the risk and magnitude of the harm that could result."[87] Recent instructions from the OMB and the DHS to federal agencies and departments point to a move toward more frequent assessments to build upon "existing continuous monitoring processes."[88]

■ Cost-Effectiveness Assessment

FISMA does not require security at all costs, but instead specifies "implementing policies and procedures to cost-effectively reduce risks to an acceptable level."[89] The NIST standards similarly identify cost effectiveness as a relevant consideration.[90] Thus, risk, cost, and efficacy all work in tandem to assist in defining a reasonable level of security, as discussed below.

■ Appropriate Level Of Security

FISMA requires a determination of "the levels of information security appropriate to protect such information and information systems in accordance with standards promulgated under [40 U.S.C.A. § 11331], for information security classifications and related requirements."[91] The "appropriate" level of security requires a certain amount of judgment, as illustrated by the implementing guidance.

(a) *Not too tight.* The security program should not be unnecessarily restrictive, according to OMB guidance: "The security required by the rules shall be only as stringent as necessary to provide adequate security for information in the system."[92]

(b) *Not too loose.* Conversely, the security program must be restrictive enough to meet the "minimum set of controls" established by the OMB and NIST standards. These minimum controls include developing a security plan with clear rules, training, personnel management, technical safeguards, periodic testing and review, and authorization procedures.[93]

(c) *Multiple factors.* The appropriate level and restrictiveness of controls depend upon multiple factors, as the NIST standards provide "flexibility to appropriately modify the controls based on specific organizational policies and requirements, particular conditions and circumstances, known threat and vulnerability information, and tolerance for risk."[94] Accordingly, the decision regarding the appropriate level of security is necessarily infused with a certain amount of business judgment.

■ Life-Cycle Security

To avoid information systems being bought without sufficient planning and budget to cover security over the long-term, FISMA requires that information security be "addressed throughout the life cycle of each agency information system."[95] Similarly, the FAR implementation recognizes "security as an important part of all phases of the IT acquisition life cycle."[96]

Implementing A Security Program

The statute and regulations provide a very top-level sketch of what defines a security program, but most of the implementing details have been left to be defined within the framework of OMB guidance and NIST standards. In particular, FISMA calls for policies and procedures that, in turn, define security controls, configuration controls, and requirements for maintaining continuity of operations.[97]

■ Policies & Procedures

An information security program requires "policies and procedures" based upon the factors described above, including risk assessments, cost-effectiveness considerations, and life-cycle factors.[98] Such "security policies, procedures, and control techniques" must "address all applicable requirements."[99] As the FAR implementation recognizes, these policies and procedures will continue to evolve "as they adapt to a dynamic IT security environment."[100]

■ Security Controls

"Security controls" are an essential part of the FISMA information security package.[101] FISMA breaks these security controls down into the categories of "management, operational, and technical controls."[102] Although FISMA does not define these controls or describe them in further detail, the NIST standards do.[103]

(1) *Management Controls.* These controls are "safeguards or countermeasures" "that focus on the management of risk and the management of information system security."[104] Examples of such controls include:[105]

(a) *Security assessment and authorization*—developing and documenting security assessment and authorization policy; identifying connections to external information systems and documenting interface characteristics, security requirements, and nature of information communicated; developing a plan of action and milestones for information systems and any remedial actions to correct weaknesses and deficiencies; and establishing a continuous monitoring strategy and program.

(b) *Risk assessment*—establishing security categories (low, moderate, high); assessing and updating risks; and performing vulnerability scanning.

(c) *Planning*—preparing a security plan and updates; establishing rules of behavior;[106] and making a privacy impact assessment.

(d) *System and services acquisition*—determining resource allocation, life cycle support, acquisition needs, system documentation, outsourcing, and related needs.

(e) *Program management*—including resources for information security program in capital planning and investment requests; developing and maintaining inventory of information systems; and documenting critical infrastructure protection plan.

(2) *Operational controls.* These controls are the "safeguards or countermeasures" "that are primarily implemented and executed by people (as opposed to systems)."[107] Examples of such controls include:[108]

(a) *Personnel security*—screening, terminating, transferring, and sanctioning personnel; preparing access agreements; and determining third-party security.

(b) *Physical and environmental security*—authorizing, controlling, and monitoring physical access; establishing visitor control and access logs; arranging for emergency shutoff, power, and lighting; and protecting against information leaks due to signals emanations.

(c) *Contingency planning*—planning, training, testing and updating contingency plans; establishing alternate sites and backup; and providing for disaster recovery.

(d) *Configuration management*—establishing configuration baseline, change control, monitoring, and settings; and restricting access for change.

(e) *Maintenance*—performing periodic, remote, and timely maintenance; and choosing maintenance tools and personnel.

(f) *System and information integrity*—maintaining intrusion detection tools, software/data integrity, and information accuracy, completeness, and validity; protecting against cyber threats; and handling errors.

(g) *Media protection*—handling media access, labeling, storage, transport, sanitization, destruction, and disposal.

(h) *Incident response*—training and testing for incident response; and handling, monitoring, and reporting incidents.

(i) *Awareness and training*—promoting security awareness; and providing and documenting training.

(3) *Technical controls*. These controls are the "safeguards or countermeasures" "that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system."[109] Examples of such controls include:[110]

(a) *Identification and authentication*—identifying and authenticating users and devices; and performing identifier and authentication management.

(b) *Access control*—managing accounts; enforcing access and information flow controls, separation of duties, and system logins; and controlling remote, wireless, portable, and mobile system access.

(c) *Audit and accountability*—identifying auditable events; determining audit storage capacity, processing, monitoring, analysis, and reporting; promoting nonrepudiation; and protecting audit information.

(d) *System and communications protection*—determining system function isolation, resource priority, boundary protection, transmission integrity and confidentiality, trusted path, cryptographic and public keys, and other system protections.

■ Continuous Monitoring

Though not expressly mentioned in FISMA, both the OMB and the DHS have emphasized continuous monitoring as an integral component of federal information security.[111] Consistent with this Executive Branch initiative, the NIST standards describe continuous monitoring of security controls as "[a] critical aspect of managing risk to information from the operation and use of information systems."[112] Effective continuous monitoring programs require integration into the organization's systems development life cycle processes.[113] In addition, continuous monitoring includes the following functions:[114]

(a) "Configuration management and control processes";

(b) "Security impact analyses on proposed or actual changes to organizational information systems and environments of operations";

(c) "Assessment of selected security controls";

(d) "Security status reporting to appropriate organizational officials"; and

(e) "Active involvement by authorizing officials in the ongoing management of information system-related security risks."

In specific guidance on continuous monitoring, NIST has identified the fundamental elements of "information security continuous monitoring (ISCM)" and defined the process for establishing, implementing, and updating such monitoring against the continually changing cyber threats and technologies.[115]

■ Configuration Control

FISMA requires policies and procedures that ensure compliance with "minimally acceptable system configuration requirements, as determined by the agency."[116] The FIPS publications also specify configuration control as integral to information and system security.[117] Configuration control is the "[p]rocess for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after system implementation."[118] Such configuration controls apply to the initial system—as well as to additions, modifications, or deletions—to define not only what is covered under the security program, but also to identify security gaps or vulnerabilities that may arise as the system evolves. The NIST standards provide guidelines to implement such configuration management security controls.[119]

■ Continuity Of Operations

Under FISMA, the "plans and procedures" must "ensure continuity of operations for information systems."[120] Such provisions would generally include

backup systems, transition plans, and security controls to maintain operations during power outages, disasters, or other interruptions to system service.

Ensuring Compliance

Once the security program is in place, the last—and continuing—duty is to assure compliance through training, periodic testing and evaluation, personal accountability, security incident detection and reporting, and remedial or corrective actions when necessary. Just as policies, procedures, and controls need to evolve to meet changing threats, so do the compliance efforts.

■ Training

To comply, people need to know and understand the rules. FISMA mandates that an "information security program" include "security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency."[121] Regarding the timing of training, the OMB standards state that mandatory training must be completed "prior to granting access to the system."[122] For such courses, the scope of training should cover the "rules of behavior" (the "responsibilities of and expectations for all individuals with access to the system"), consider the NIST standards, and address the "consequences of non-compliance."[123] In addition, the OMB rules contemplate refresher training: "[o]ver time, attention to security tends to dissipate."[124] Accordingly, "individuals should periodically have refresher training to assure that they continue to understand and abide by the applicable rules."[125]

■ Periodic Testing & Evaluation

FISMA provides for "periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented."[126] The scope of such testing must cover the "management, operational, and technical controls of every information system identified in the inventory."[127]

The frequency of such testing and evaluation depends upon the risk, but FISMA mandates that such actions be performed at least annually.[128] The requirement for annual testing may be satisfied by the "independent evaluation of the information security program and practices" that is required by FISMA.[129]

However, a number of critics have complained that an annual review process failed to promote security, but instead pushed agencies towards a box-checking "paperwork" exercise that did not keep current with expanding and morphing cyber threats.[130] More recently, the OMB and the DHS have placed greater emphasis upon continuous monitoring, rather than annual evaluation.[131] The current NIST standards also emphasize the importance of continuous monitoring as an essential element of a federal information security program:[132]

> [The Risk Management Framework]... [p]romotes the concept of near real-time risk management and ongoing information system authorization through the implementation of robust continuous monitoring processes[.]

■ Accountability

Under FISMA, focused management attention is required for information security. In particular, the Chief Information Officer (CIO) must designate a "senior…information security officer" who must have the necessary "professional qualifications," "have information security duties as [the] official's primary duty," and "head an office" with the mission and resources to enforce compliance.[133] Such accountability is reinforced by the requirement for an annual independent evaluation.[134]

■ Security Incident Detection & Reporting

In anticipation of security breaches or "incidents," FISMA requires "procedures for detecting, reporting, and responding to security incidents," including procedures for "mitigating risks associated with such incidents before substantial damage is done."[135] The OMB has issued guidance regarding responses to, and reporting of, security breaches.[136] Similarly, NIST has issued a detailed guide for responding to security incidents and breaches.[137]

■ Remedial Actions

When a security program noncompliance occurs, a process must exist for taking corrective

or remedial action—"a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency."[138] In a continuous monitoring program, the agency or contractor employs real-time data of security incidents or breaches to update its security protocols and to tailor its defenses to the changing security threats.[139]

GUIDELINES

These *Guidelines* are intended to assist you in understanding the risks and rules relating to federal information security for agencies and contractors. They are not, however, a substitute for professional representation in any specific situation.

1. *Know your data.* Identify your high-value data (including personally identifiable information, healthcare data, and trade secrets) and prioritize your information security program to focus more effort on protecting your most critical information.

2. *Identify the risks.* Track the latest threats through available Government sources, public-private partnerships, and/or industry data and update your information security defenses to counter the evolving strategies and technology of hackers seeking to break into your systems and data banks.

3. *Review your interconnections and data sharing.* When you share data with other parties and interconnect with other systems, assure that you have security controls and specific agreements defining the security protocols and allocation of risk between the parties for such sharing and interconnections.

4. *Monitor continuously.* Just as the Maginot line did not work against traditional threats in World War II, static security plans and defenses certainly will fail in cyberspace, thus requiring continuous monitoring as an essential part of effective information security.

5. *Involve the whole organization.* Information security is not just an IT department function, but instead must be borne by the organization at the highest management levels, including the financial officers and lawyers, because effective information security requires dedicated resources and full management commitment in order to work.

6. *Train, train, train.* Many security vulnerabilities can be closed simply by assuring that personnel accessing IT systems and sensitive data understand the nature of the risks, the applicable rules, and the importance of applying sound security principles on a daily basis.

7. *Remember mobile devices.* As organizations shift from desktops to laptops to mobile devices, the security perimeter continues to expand, thus requiring organizations to update security controls and procedures to account for the expanding risks associated with mobile devices.

★ REFERENCES ★

1/ Cybersecurity: Next Steps To Protect Our Critical Infrastructure: Hearing Before the S. Comm. on Commerce, Science & Transportation, 111th Cong. (Feb. 23, 2010) (statement of Vice Adm. McConnell), http://commerce.senate.gov/public/?a=Files.Serve&File_id=52507485-dfbe-4873-8089-82dd24f7beaa.

2/ White House Office of the Press Secretary, Remarks by the President on Securing Our Nation's Cyber Infrastructure (May 29, 2009), http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

3/ White House Office of the Press Secretary, Remarks by the President on Securing Our Nation's Cyber Infrastructure (May 29, 2009), http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

4/ Cybersecurity: Next Steps To Protect Our Critical Infrastructure: Hearing Before the S. Comm. on Commerce, Science & Transportation, 111th Cong. (Feb. 23, 2010) (statement of Sen. Rockefeller) ("A major 'cyberattack' could shut down our nation's most critical infrastructure…."), http://commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=a676548f-a2a7-40ff-a18d-889a7907801c&Statement_id=4907648b-ac7b-4263-9cbf-188f0618f7b4&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=b06c39af-e033-4cba-9221-de668ca1978a&MonthDisplay=2&YearDisplay=2010; Senate Comm. on Commerce, Science & Transportation, Press Release, Rockefeller and Snowe Gain Momentum for Landmark Cybersecurity Act (Mar. 24, 2010) (statement of Sen. Snowe) ("cyber

intrusions and attacks represent both a potential national security and economic catastrophe"), http://commerce.senate.gov/public/index.cfm?p=PressReleases&ContentRecord_id=3a0945bb-d5d8-47f4-a86c-2f71f15892bd&ContentType_id=77eb43da-aa94-497d-a73f-5c951ff72372&Group_id=4b968841-f3e8-49da-a529-7b18e32fd69d&MonthDisplay=3&YearDisplay=2010.

5/ Marshall, "Panetta Discusses Security Challenges in Stratcom Visit," American Forces Press Service, Aug. 5, 2011, http://www.defense.gov/news/newsarticle.aspx?id=64946.

6/ OMB, FY 2005 Report to Congress on Implementation of the E-Government Act of 2002, at 5 (Mar. 1, 2006), http://georgewbush-whitehouse.archives.gov/omb/inforeg/reports/2005_e-gov_report.pdf; see also OMB, FY 2006 Report to Congress on Implementation of the E-Government Act of 2002, at 3 (Mar. 1, 2007), http://georgewbush-whitehouse.archives.gov/omb/inforeg/reports/2006_egov_report.pdf; OMB Circular A-130 Revised, Transmittal Memorandum No. 4, § 7(a), http://www.whitehouse.gov/omb/circulars_a130_a130trans4.

7/ Hearing on Draft Legislative Proposal on Cybersecurity: Hearing Before the Subcomm. on Cybersecurity, Infrastructure Protection & Security Technologies of the H. Comm. on Homeland Security, 112th Cong. (Dec. 6, 2011) (statement of Rep. Lungren), http://homeland.house.gov/hearing/subcommittee-hearing-hearing-draft-legislative-proposal-cybersecurity.

8/ White House Cyberspace Policy Review 26 (May 2009), http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf; see also White House Cyberspace Policy Review 38 (May 2009), http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf ("Develop mechanisms for cybersecurity-related information sharing…."); White House Cybersecurity Legislative Proposal, "Section 1, Department of Homeland Security Cybersecurity Authority" 3 (May 12, 2011) (proposing to amend Title II of the Homeland Security Act of 2002, 6 U.S.C.A. § 121 et seq., by adding a new Subtitle E, § 243(c)(5)(A)) ("facilitate information sharing, interaction and collaboration among and between agencies; State, local, tribal and territorial governments; the private sector; academia and international partners"), http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/dhs-cybersecurity-authority.pdf.

9/ Hearing on Draft Legislative Proposal on Cybersecurity: Hearing Before the Subcomm. on Cybersecurity, Infrastructure Protection & Security Technologies of the H. Comm. on Homeland Security, 112th Cong. (Dec. 6, 2011) (statement of Rep. Lungren), http://homeland.house.gov/hearing/subcommittee-hearing-hearing-draft-legislative-proposal-cybersecurity.

10/ Hearing on Draft Legislative Proposal on Cybersecurity: Hearing Before the Subcomm. on Cybersecurity, Infrastructure Protection & Security Technologies of the H. Comm. on Homeland Security, 112th Cong. (Dec. 6, 2011) (statement of Cheri McGuire, Symantec Corp.) ("Information sharing is often referred to as the key to combating cyber threats"), http://homeland.house.gov/hearing/subcommittee-hearing-hearing-draft-legislative-proposal-cybersecurity; Private Sector Perspectives on Department of Defense Information Sharing Technology and Cybersecurity Activities: Hearing Before the Subcomm. on Terrorism, Unconventional Threats & Capabilities of the H. Comm. on Armed Services, 111th Cong. (Feb. 25, 2010) (statement of David Bodenheimer summarizing private sector perspectives on information sharing and cybersecurity).

11/ Information Sharing in the Era of WikiLeaks: Balancing Security and Collaboration: Hearing Before the S. Comm. on Homeland Security & Government Affairs, 112th Cong. (Mar. 10, 2011) (statement of Sen. Collins), http://www.hsgac.senate.gov/hearings/information-sharing-in-the-era-of-wikileaks-balancing-security-and-collaboration.

12/ Center for Strategic & International Studies Commission on Cybersecurity, Securing Cyberspace for the 44th Presidency 12–13 (Dec. 2008), http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

13/ H. Comm. on Science, Space & Technology, Subcommittee Chairman Lipinski's Floor Speech on H.R. 4061 (Feb. 3, 2010), http://archives.democrats.science.house.gov/press/PRArticle.aspx?NewsID=2736.

14/ Sen. Comm. on Homeland Security & Governmental Affairs, News Release, Lieberman, Collins, Carper Introduce Bill To Address Serious Cyber Security Threats (Feb. 17, 2011) (remarks by Sen. Collins), http://www.hsgac.senate.gov/subcommittees/federal-financial-management/majority-media/-lieberman-collins-carper-introduce-bill-to-address-serious-cyber-security-threats.

15/ Cybersecurity: Assessing the Nation's Ability To Address the Growing Cyber Threat: Hearing Before the H. Comm. on Oversight & Government Reform, 112th Cong. (July 7, 2011) (statement of Rep. Issa), http://oversight.house.gov/index.php?option=com_content&view=article&id=1363%3A7-7-11-qcybersecurity-assessing-the-nations-ability-to-address-the-growing-cyber-threatq&catid=12&Itemid=20.

16/ Center for Strategic & International Studies Commission on Cybersecurity, Securing Cyberspace for the 44th Presidency 11 (Dec. 2008), http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

17/ Congressional Research Service, Report R40427, Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations 3 (Mar. 10, 2009).

18/ White House Office of the Press Secretary, Remarks by the President on Securing Our Nation's Cyber Infrastructure (May 29, 2009), http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

19/ "Source in Iran Sees Plans for President's Chopper," USA Today, Mar. 2, 2009.

20/ Cybersecurity: Assessing the Nation's Ability To Address the Growing Cyber Threat: Hearing Before the H. Comm. on Oversight & Government Reform, 112th Cong. (July 7, 2011) (statement of Rep. Issa), http://oversight.house.gov/index.php?option=com_content&view=article&id=1363%3A7-7-11-qcybersecurity-assessing-the-nations-ability-to-address-the-growing-cyber-threatq&catid=12&Itemid=20.

21/ White House Cyberspace Policy Review at i (May 2009), http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

22/ Do the Payment Card Industry Data Standards Reduce Cybercrime? Hearing Before the Subcomm. on Emerging Threats, Cybersecurity & Science and Technology of H. Comm. on Homeland Security, 111th Cong. (Mar. 31, 2009) (statement of Chairman Thompson), http://www.homelandsecurity.house.gov/SiteDocuments/20090331141926-86082.pdf.

23/ Whitehouse, "We Need to Act on Cybersecurity," Nat'l L.J., May 10, 2010.

24/ The Cybersecurity Act of 2010, S.773, 111th Cong., § 2(8) (2010), http://www.gpo.gov/fdsys/pkg/BILLS-111s773rs/pdf/BILLS-111s773rs.pdf; see also Congressional Research Service, Report R40427, Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations 3 (Mar. 10, 2009) (potential for "strategic damage to the United States"); Wright, "The Spymaster: Can Mike McConnell fix America's Intelligence Community?," The New Yorker, Jan. 21, 2008, at 51 ("McConnell then said, 'If the 9/11 perpetrators had focused on a single U.S. bank through cyber-attack and it had been successful, it would have an order-of-magnitude greater impact on the U.S. economy.'").

25/ Perlroth, "Insurance Against Cyber Attacks Expected To Boom," N.Y. Times, Dec. 23, 2011, http://bits.blogs.nytimes.com/2011/12/23/insurance-against-cyber-attacks-expected-to-boom/.

26/ Data Security and Breach Notification Act of 2010: Hearing on S.3742 Before the Subcomm. on Consumer Protection, Product Safety & Insurance of the S. Comm. on Commerce, Science & Transportation, 111th Cong. (Sept. 22, 2010) (statement of Ioana Rusu, Policy Counsel, Consumers Union), http://commerce.senate.gov/public/?a=Files.Serve&File_id=8452abd6-4671-49e8-a117-68b6f85c5a2d.

27/ The Threat of Data Theft to American Consumers: Hearing Before the Subcomm. on Commerce, Manufacturing & Trade of the H. Comm. on Energy & Commerce, 112th Cong. (May 4, 2011) (Majority Committee Staff Internal Memorandum), http://energycommerce.house.gov/hearings/hearingdetail.aspx?NewsID=8534; see also Privacy Rights Clearinghouse, Chronology of Data Breaches, http://www.privacyrights.org/data-breach .

28/ Kime, "DOD Hit With Lawsuit Over Lost Tricare Data," ArmyTimes, Oct. 13, 2011, http://www.armytimes.com/news/2011/10/military-dod-hit-with-lawsuit-over-lost-tricare-data-101311/.

29/ S. Rep. No. 111-110, at 3 (Dec. 17, 2009).

30/ Chabrow, "Navy CIO's PII Exposed for Sixth Time," Gov't Info. Sec. News, Jan. 4, 2010, http://blogs.govinfosecurity.com/posts.php?postID=404&rf=010510eg.

31/ Cybersecurity: Assessing Our Vulnerabilities and Developing an Effective Response: Hearing Before the S. Comm. on Commerce, Science &

Transportation, 111th Cong. 8 (Mar. 19, 2009) (statement of Dr. James Lewis), http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_senate_hearings&docid=f:50638.pdf.

32/ 44 U.S.C.A. §§ 3541–49.

33/ 44 U.S.C.A. § 3541(1). Congress intended FISMA to consolidate and clarify several statutory regimes "to guide Federal agencies to provide needed improvements to their information security." H.R. Rep. No. 107-787, at 54 (2002), reprinted in 2002 U.S.C.C.A.N. 1880, 1889.

34/ 44 U.S.C. A. § 3543(a).

35/ 44 U.S.C.A. § 3543(b), (c).

36/ 44 U.S.C.A. § 3544.

37/ 44 U.S.C.A. § 3544.

38/ 44 U.S.C.A. § 3545.

39/ 44 U.S.C.A. § 3544(a) (emphasis added); see also 44 U.S.C.A. § 3544(b) (including information systems "provided or managed by…contractor, or other source").

40/ 5 U.S.C.A. § 552a.

41/ 5 U.S.C.A. § 552a(a), (b). The Privacy Act contains a number of exceptions and exemptions, such as internal agency distribution, routine use, certain law enforcement purposes, "compelling circumstances" involving health or safety, or congressional access. See, e.g., 5 U.S.C.A. § 552a(b), (j), (k).

42/ 5 U.S.C.A. § 552a(g), (i).

43/ Schwartz, "6 Worst Data Breaches of 2011," Info. Wk., Dec. 28, 2011, http://informationweek.com/news/security/attacks/232301079?queryText=6+Worst+Data+Breaches+of+2011.

44/ 5 U.S.C.A. § 552a(m).

45/ 5 U.S.C.A. § 552a(m)(1); Unt v. Aerospace Corp., 765 F.2d 1440, 1447 (9th Cir. 1985).

46/ 5 U.S.C.A. § 552a(m)(1); FAR 52.224-2.

47/ See, e.g., Congressional letter to DOD TRICARE Management Authority (Dec. 2, 2011) regarding SAIC's loss of data for 4.9 million patients, http://patientprivacyrights.org/wp-content/uploads/2011/12/12-2-2011-SAIC-Oversight-Letter.pdf.

48/ FAR 7.103(w).

49/ FAR 39.101(d).

50/ FAR 39.105.

51/ FAC 2005-06, 70 Fed. Reg. 57449, 57451 (Sept. 30, 2005).

52/ 70 Fed. Reg. at 57450.

53/ 48 C.F.R. §§ 539.7001–7002.

54/ 48 C.F.R. §552.239-71, para. (a).

55/ See 77 Fed. Reg. 749, 750 (Jan. 6, 2012). The GSA security requirements clause (48 C.F.R. § 552.239-71, para. (b)) expressly requires the contractor to comply with the CIO IT Security Procedural Guide 09-48, http://www.gsa.gov/portal/category/25690.

56/ 48 C.F.R. §552.239-71, para. (d).

57/ 48 C.F.R. § 552.239-71, para. (e).

58/ 48 C.F.R. § 552.239-71, para. (f).

59/ 48 C.F.R. § 552.239-71, para. (j).

60/ 48 C.F.R. § 552.239-71, para. (k).

61/ FISMA establishes exceptions to its scope for "national security systems." 44 U.S.C.A. § 3542(b).

62/ DFARS 239.7102-1.

63/ See, e.g., DOD Instruction 8510.01 (Nov. 28, 2007), http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf).

64/ 48 C.F.R. § 3052.204-70 (applicable to "all systems connected to a DHS network or operated by the Contractor for DHS" or to instances where the contractor will have "physical or electronic access to sensitive information contained in DHS unclassified systems").

65/ 48 C.F.R. § 352.239-72 (applicable to "information technology resources or services in which the Contractor has physical or logical (electronic) access to, or operates a Department of Health and Human Services (HHS) system containing information that directly supports HHS' mission").

66/ 48 C.F.R. § 952.204-77; see 48 C.F.R. § 904.404(d)(7) (making the clause applicable where "the contractor may have access to computers owned, leased or operated on behalf of the Department of Energy").

67/ VA Acquisition Regulation (VAAR) 852.273-75 (applicable where "VA information and/or Information Technology will be accessed or utilized").

68/ 44 U.S.C.A. § 3544(b)(2)(D).

69/ 40 U.S.C.A. § 11331(b)(1)(C) (emphasis added).

70/ FAR 7.103(w).

71/ FAC 2005-06, 70 Fed. Reg. 57449, 57450 (Sept. 30, 2005); see also FAR 11.201(d)(4) (referencing FIPS publications).

72/ OMB Memorandum 10-28, Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS) (July 6, 2010), http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-28.pdf.

73/ OMB Memorandum 11-33, FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (Sept. 14, 2011) (enclosing DHS Memorandum FISM 11-02 (Aug. 24, 2011)), http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-33.pdf.

74/ OMB Memorandum 11-33, FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (Sept. 14, 2011) (enclosing DHS Memorandum FISM 11-02 (Aug. 24, 2011)), http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-33.pdf.

75/ OMB Memorandum 11-33, FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (Sept. 14, 2011) (enclosing DHS Memorandum FISM 11-02 (Aug. 24, 2011)), http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-33.pdf.

76/ 44 U.S.C.A § 3542(b)(1); see also FAR 2.101(b); 70 Fed. Reg. 57449, 57451 (Sept. 30, 2005).

77/ FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems 1, § 2 (Feb. 2004), http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf. FAR 11.102 and 11.201 include references to the FIPS PUB standards.

78/ 44 U.S.C.A. § 3542(b)(1)(A); FAR 2.101(b). "Nonrepudiation" is the "[p]rotection against an individual falsely denying having performed a particular action" and "[p]rovides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message." "Authenticity" means "[t]he property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator." NIST Special Publication 800-53, Rev. 3, Recommended Security Controls for Federal Information Systems, App. B, at B-1, B-9 (May 2010), http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

79/ 44 U.S.C.A. § 3542(b)(1)(B); FAR 2.101(b).

80/ 44 U.S.C.A. § 3542(b)(1)(C); FAR 2.101(b).

81/ 44 U.S.C.A. § 3544(a)(3)(C).

82/ 44 U.S.C.A. § 3544(b)(2)(D).

83/ See, e.g., OMB Circular A-130 Revised, Transmittal Memorandum No. 4, App. III, "Security of Federal Automated Information Resources," http://www.whitehouse.gov/omb/circulars_a130_a130appendix_iii; NIST information security publications, such as Special Publication 800-53A, Rev. 1, Guide for Assessing the Security Controls in Federal Information Systems (June 2010), http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf; see also FAR 7.103(w) (expressly referencing "OMB's implementing policies including Appendix III of OMB Circular A-130, and guidance and standards from the Department of Commerce's National Institute of Standards and Technology"); FAC 2005-06, 70 Fed. Reg. 57449, 57451 (Sept 30, 2005) (contemplating the applicability of the OMB guidance and NIST standards to contractors in referencing "associated implementing guidance from the Office of Management and Budget (OMB) and National Institute of Standards and Technology, particularly FISMA's requirement for agencies to ensure contractor compliance with all current IT security laws and policies").

84/ 44 U.S.C.A. § 3544(a)(2)(A).

85/ 44 U.S.C.A. § 3544(b)(2)(A).

86/ FAC 2005-06, 70 Fed.Reg.57449, 57450–51 (Sept. 30, 2005); see also NIST Special Publication 800-30, Rev. 1 (Draft), Guide for Conducting Risk Assessments (Sept. 2011) (discussion of methods and factors for conducting risk assessments), http://csrc.nist.gov/publications/drafts/800-30-rev1/SP800-30-Rev1-ipd.pdf; FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems (Feb. 2004) (guidelines for assessing risk for security breaches), http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

87/ 44 U.S.C.A. § 3544(b)(1).

88/ OMB Memorandum 11-33, FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (Sept. 14, 2011) (enclosing DHS Memorandum FISM 11-02 (Aug. 24, 2011)), http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-33.pdf.

89/ 44 U.S.C.A. § 3544(a)(2)(C); see also 44 U.S.C.A. § 3544(b)(2)(B).

90/ NIST Special Publication 800-53A, Rev. 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations 3, § 1.1 (June 2010) ("[O]rganizations have the inherent flexibility to determine the level of effort needed for a particular assessment….This determination is made on the basis of what will accomplish the assessment objectives in the most cost-effective manner and with sufficient confidence to support the subsequent determination of the resulting mission or business risk."), http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf.

91/ 44 U.S.C. § 3544(a)(2)(B). FISMA (44 U.S.C.§ 3544(a)(2)(B)) includes an express reference to 40 U.S.C.A. § 11331, which expressly refers to NIST standards and then states that "Information security standards described under subparagraph (B) shall be compulsory and binding." 40 U.S.C. § 11331(b)(1)(C).

92/ OMB Circular A-130 Revised, Transmittal Memorandum No. 4, App. III, § A(3)(a)(2)(a), http://www.whitehouse.gov/omb/circulars_a130_a130appendix_iii.

93/ OMB Circular A-130 Revised, Transmittal Memorandum No. 4, App. III, § A(3)(a)–(b), http://www.whitehouse.gov/omb/circulars_a130_a130appendix_iii.

94/ NIST Special Publication 800-53, Rev. 3, Recommended Security Controls for Federal Information Systems and Organizations 4, § 1.4 (May 2010), http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf; see also NIST Special Publication 800-53, Rev. 3, Recommended Security Controls for Federal Information Systems and Organizations 2, § 1.1 (May 2010) (The guidelines… [p]rovide a stable, yet flexible catalog of security controls for information systems and organizations to meet current organizational protection needs and the demands of future protection needs based on changing requirements and technologies[.]"), http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf; NIST Special Publication 800-53A, Rev. 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations 3, § 1.1 (June 2010) ("The use of Special Publication 800-53A… offers the needed flexibility to customize the assessment based on organizational policies and requirements, known threat and vulnerability information, operational considerations, information system and platform dependencies, and tolerance for risk."), http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf.

95/ 44 U.S.C.A. § 3544(b)(2)(C).

96/ See FAC 2005-06, 70 Fed.Reg.57450 (Sept. 30, 2005).

97/ 44 U.S.C.A. § 3544(b).

98/ 44 U.S.C.A. § 3544(b)(2); NIST Special Publication 800-53, Rev. 3, Recommended Security Controls for Federal Information Systems and Organizations 4–5, § 1.4 (May 2010), http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf; NIST Special Publication 800-64, Security Considerations in the System Development Life Cycle 1 (Oct. 2008), http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf.

99/ 44 U.S.C.A. § 3544(a)(3)(C).

100/ FAC 2005-06, 70 Fed. Reg. 57449, 57450 (Sept. 30, 2005).

101/ 44 U.S.C.A. § 3544(a)(2)(D).

102/ 44 U.S.C.A. § 3544(b)(5)(A).

103/ See, e.g., NIST Special Publication 800-53, Rev. 3, Recommended Security Controls for Federal Information Systems and Organizations 6, § 2.1 (May 2010), http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

104/ NIST Special Publication 800-53, Rev. 3, Recommended Security Controls for Federal Information Systems and Organizations, App. B, at B-7 (May 2010), http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf; NIST Special Publication 800-53A, Rev. 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations, App. B, at B-6 (June 2010), http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf.

105/ NIST Special Publication 800-53A, Rev. 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations, App. F (June 2010), http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf.

106/ "Rules of behavior" should "clearly delineate responsibilities of and expectations for all individuals with access to the system," "state the consequences of non-compliance," and "form the basis for security awareness and training." OMB Circular A-130, Revised, Transmittal Memorandum No. 4, App. III, § B(a)(2), http://www.whitehouse.gov/omb/circulars_a130_a130appendix_iii.

107/ NIST Special Publication 800-53A, Rev. 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations, App. B, at B-7 (June 2010), http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf.

108/ NIST Special Publication 800-53, Rev. 3, Recommended Security Controls for Federal Information Systems and Organizations 6, § 2.1 (May 2010), http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf; NIST Special Publication 800-53A, Rev. 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations, App. F (June 2010), http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf.

109/ NIST Special Publication 800-53A, Rev. 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations, App. B, at B-11 (June 2010), http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf.

110/ NIST Special Publication 800-53, Rev. 3, Recommended Security Controls for Federal Information Systems and Organizations 6, § 2.1 (May 2010), http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf; NIST Special Publication 800-53A, Rev. 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations, App. F (June 2010), http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf.

111/ OMB Memorandum 11-33, FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (Sept. 14, 2011) (enclosing DHS Memorandum FISM 11-02 (Aug. 24, 2011)), http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-33.pdf.

112/ NIST Special Publication 800-37, Rev. 1, Guide for Applying the Risk Management Framework to Federal Information Systems, App. G, at G-1 (Feb. 2010), http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.

113/ NIST Special Publication 800-37, Rev. 1, Guide for Applying the Risk Management Framework to Federal Information Systems, App. G, at G-1 (Feb. 2010), http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.

114/ NIST Special Publication 800-37, Rev. 1, Guide for Applying the Risk Management Framework to Federal Information Systems, App. G, at G-2 (Feb. 2010), http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.

115/ NIST Special Publication 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations (Sept. 2011), http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf.

116/ 44 U.S.C.A. § 3544(b)(2)(D)(iii).

117/ FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems at 2, § 3 (Mar. 2006), http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.

118/ NIST Special Publication 800-53, Rev. 3, Recommended Security Controls for Federal Information Systems and Organizations, App. B, at B-3 (May 2010), http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

119/ NIST Special Publication 800-128, Guide for Security-Focused Configuration Management of Information Systems (Aug. 2011), http://csrc.nist.gov/publications/nistpubs/800-128/sp800-128.pdf.

120/ 44 U.S.C.A. § 3544(b)(8).

121/ 44 U.S.C.A. § 3544(b)(4); see also 44 U.S.C.A. § 3544(a)(3)(D) ("training"); OMB Circular A-130 Revised, Transmittal Memorandum No. 4, App. III, § B(a)(2)(b) ("mandatory periodic training"), http://www.whitehouse.gov/omb/circulars_a130_a130appendix_iii; NIST Standard Publication 800-50, Building an Information Technology Security Awareness and Training Program (Oct. 2003), http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.

122/ OMB Circular A-130, Revised, Transmittal Memorandum No. 4, App. III, § B(a)(2)(b) ("The Appendix enforces such mandatory training by requiring its completion prior to granting access to the system."), http://www.whitehouse.gov/omb/circulars_a130_a130appendix_iii.

123/ OMB Circular A-130, Revised, Transmittal Memorandum No. 4, App. III, http://www.whitehouse.gov/omb/circulars_a130_a130appendix_iii.

124/ OMB Circular A-130, Revised, Transmittal Memorandum No. 4, App. III, § B(a)(2)(b), http://www.whitehouse.gov/omb/circulars_a130_a130appendix_iii.

125/ OMB Circular A-130, Revised, Transmittal Memorandum No. 4, App. III, § B(a)(2)(b), http://www.whitehouse.gov/omb/circulars_a130_a130appendix_iii.

126/ 44 U.S.C.A. § 3544(a)(2)(D).

127/ 44 U.S.C.A. § 3544(b)(5)(A).

128/ 44 U.S.C.A. § 3544(b)(5).

129/ See 44 U.S.C.A § 3545(a) referenced in 44 U.S.C.A. § 3544(b)(5)(B).

130/ More Security, Less Waste: What Makes Sense for Our Federal Cyber Defense: Hearing Before the Subcomm. on Federal Financial Management, Government Information, Federal Services & International Security, 111th Cong. (Oct. 29, 2009) (statement of Sen. McCain), http://www.hsgac.senate.gov/subcommittees/federal-financial-management/hearings/more-security-less-waste-what-makes-sense-for-our-federal-cyber-defense_- .

131/ As a reflected in the Executive Branch's most recent guidance on FISMA monitoring and reporting, the focus has "shift[ed] from the once-a-year FISMA reporting process to a monthly reporting of key metrics…." OMB Memorandum 11-33, FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (Sept. 14, 2011) (enclosing DHS Memorandum FISM 11-02 (Aug. 24, 2011)), http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-33.pdf.

132/ NIST Special Publication 800-37, Rev. 1, Guide for Applying the Risk Management Framework to Federal Information Systems at 2, § 1.1 (Feb. 2010), http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf; see also NIST Special Publication 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations (Sept. 2011), http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf.

133/ 44 U.S.C. § 3544(a)(3)(A).

134/ 44 U.S.C.A. § 3545(a).

135/ 44 U.S.C.A. § 3544(b)(7).

136/ OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007), http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf.

137/ NIST Special Publication 800-61, Rev. 1, Computer Security Incident Handling Guide (Mar. 2008), http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf.

138/ 44 U.S.C.A. § 3544(b)(6); see also 44 U.S.C.A. § 3544(a)(5) (annual reporting on effectiveness of security program, "including progress of remedial actions").

139/ See, e.g., NIST Special Publication 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations (Sept. 2011), http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf.