Statement of

Christopher E. Fountain
President and CEO
SecureInfo Corporation

Concerning

Federal Information Security: Current Challenges and Future Policy Considerations

Before the

Subcommittee on Government Management, Organization, and Procurement
Committee on Oversight and Government Reform
U.S. House of Representatives

Chair Watson, Ranking Member Bilbray, members of the subcommittee, thank you for the opportunity to provide testimony today regarding the current challenges facing the Federal government information security. My name is Chris Fountain. I am president and chief executive officer of SecureInfo Corporation.

SecureInfo is focused exclusively on providing information assurance and cyber security solutions to the Federal government. We help to secure information assets used by the Department of Homeland Security, the Department of Defense, and many other government agencies. We also provide these services to commercial organizations doing business with the Federal government.

In my testimony, I will address two primary topics: (i) what elements of the current FISMA legislation are working and should not be changed; and (ii) what changes and enhancements should be considered in future legislation.

General Background

This Committee created FISMA, and in so doing provided a framework to protect information technology (IT) infrastructure and secure data used across government. It provided this framework at a time when the general public was not aware of or concerned about information or cyber security.

Much has changed in the seven plus years since this law was enacted. Today, information systems, and the data they store, process, organize and manage, are central to everyday life and are more interconnected than ever. These “information assets" perform tasks as mundane as completing a phone call and as complex as controlling the reactor inside a nuclear power plant. They may contain something as simple as the date and time of someone's next dentist appointment or as mission critical as the launch sequence required to put a missile on target in a military engagement.

The United States government performs more critical missions enabled by networked information assets and holds more sensitive data than any other entity in the world. And, now more than ever, our adversaries actively seek to exploit our dependence on information assets. This puts an extraordinary burden on those working within and on behalf of our government and places an extremely high level of importance on securing information assets under the control of government.

When the 107th Congress established FISMA in law, it established an essential roadmap for the Federal government. While FISMA has been successful in improving the security posture of the Federal government’s information assets, changes under consideration by this subcommittee are timely and critical.

What Elements of FISMA Are Working

General information security awareness – FISMA has contributed to a heightened awareness about the importance of information security and a disciplined approach to managing it. Training requirements under FISMA anchored the law's disciplined framework across government and ensured that security was a priority in any IT system's creation or evolution. The Department of Defense has taken this a step further and now requires specific certifications for those charged with management and administration of information assets.

Executive level accountability across all government agencies – FISMA holds the head of each agency and its chief information officer accountable for implementing policies and procedures to reduce information security risks. Senior information technology leaders focused on information security are now in place across government to support these efforts and report regularly the state of information security programs within their respective agencies.

Comprehensive information security standards and guidelines – A cornerstone of FISMA was to require the implementation and ongoing maintenance of standards and guidelines to be used by the Federal government to secure information systems. The National Institute of Standards and Technology (NIST) was directed to lead this effort for Federal civilian government agencies. As a result, the Federal government now possesses one of the most complete sets of information security standards, guidance and best practices available. This work has been so successful that the Committee for National Security Systems (CNSS) in collaboration with NIST has decided to utilize updated versions of the NIST framework for Department of Defense (DOD) and Intelligence Community (IC) systems. Highlighted below are two major NIST Special Publication updates that resulted from intense collaboration between members of the NIST, CNSS, DOD and IC organizations. The acknowledgements page from SP 800-37 Revision 1 document is attached as Exhibit 1.

- NIST introduced in August, 2009: Special Publication 800-53 Revision 3, “Recommended Security Controls for Federal Information Systems and Organizations”
- NIST introduced in February, 2010: Special Publication 800-37 Revision 1, “Guide for Applying the Risk Management Framework to Federal Information Systems”

FISMA empowered NIST to develop and maintain a comprehensive suite of publications designed to help the United States government effectively and appropriately manage information security risk. NIST has proven it is highly effective at collaborating with government and industry to evolve as technology and threat vectors change. I strongly encourage this sub-committee to avoid proposing legislation that dilutes or otherwise negatively impacts NIST’s key role as provided in current FISMA legislation.

Where Does FISMA Fall Short

FISMA reporting is too focused on compliance demonstration – Today, FISMA reporting to OMB and the Congress is about compliance demonstration, rather than about an assessment of the real information security posture of information assets used by government agencies. The distinction between FISMA in broad terms and FISMA reporting is important because some would argue that "FISMA" is a paperwork exercise and does not effectively improve an agency's information security posture. I would disagree. While the reporting process is too focused on compliance demonstration, the documentation related to key information security program elements, as required by standards and guidance driven by FISMA, is important and is central to the effective governance of information assets.

Since in my view FISMA reporting needs to be more performance-based, any new legislation should address how Federal agency information security programs are assessed or graded. This problem can be solved by developing and implementing a standardized and quantitative performance-based assessment program to determine whether information assets are truly secure. The assessment program should be performed using a priority scheme driven by mission impact and should utilize a sampling process. It should include simulated attacks as well as a deep inspection of key information security program elements. These assessments should be performed by highly skilled and credentialed assessors authorized to work across government. This would help to ensure consistency and objectivity.

FISMA lacks centralized authority and a statutory basis for assessing compliance – Today, FISMA lacks a strong enforcement and oversight mechanism, which I believe this legislation addresses through creation of an empowered, Senate-confirmed, dedicated office and senior cyber executive. In creating this office, the legislation envisions a stricter FISMA compliance discipline than exists today where no significant consequences result from inadequate agency adherence.

The previous basis to encourage compliance, in no small way, was built upon the non-statutory report card process initiated and overseen by this Committee. Congressional oversight constitutes a big stick and the impact of the report card process on agency compliance was substantial, but a statute ensures longer-term and more predictable compliance. Absent a statute and corresponding budget resources, FISMA runs the risk of inadequate enforcement, and hence, compliance. I believe the statute and Committee report card process are compatible. In fact, the Committee's work encouraged agencies to seek better grades. I would encourage the Committee to revisit that process as outlined above.

The office envisioned by this legislation, the National Office for Cyberspace, with statutory authority to work across government, is sound. It is a reasoned and needed evolution of a law whose enactment rationale is more important today than ever. In creating the office, Congress can put power in such a position and FISMA provides the framework and logical opportunity to achieve this.

Placement of such an office may precipitate debate in both the Congress and Executive Branch. I would encourage the Committee to consider placing the National Office for Cyberspace within the Department of Homeland Security. Its jurisdiction touches government-wide Federal operations, state and local

jurisdictions and the private sector as well. Cyber security is about homeland security, whether the threats be from terrorists or foreign nationals seeking mass destruction, theft of military secrets or damage to our economy through an array of imaginable and frightening scenarios. It should be noted that today DHS houses the National Cyber Security Division (NCSD). NCSD carries the charter for working with the private sector to ensure our nation's critical infrastructure is effectively resistant to a cyber attack. In addition NCSD works with our international partners as cyber security is by definition a global issue. Working together, the National Office for Cyberspace and NCSD will be well positioned to address cyber security needs across Federal, state and local governments, private sector organizations involved with our critical infrastructure, and our international partners. This, together with the Committee's legislation to create a dedicated office with an empowered senior executive at its head, offers a powerful combination of statutory authority and ability to collaborate to mitigate risks associated with information technology vulnerabilities, today and well into the future.

In summary, statutory changes prescribing standards-based performance requirements and accountability through a dedicated office and official, with regular reporting to the Secretary of Homeland Security, President and Legislative Branch will ensure discipline and compliance by agencies across government. Such an office is timely, and frankly, overdue. I am encouraged by the Committee's legislation and hope my perspective contributes to your work. This issue is of greater importance than many of us recognize. Our information assets are under attack every day. It is imperative that we make every effort to properly protect them.

Closing

Thank you for the opportunity to testify and present these views. I look forward to answering any questions you might have today or in the weeks ahead as your legislative initiative progresses.

Exhibit 1, Acknowledgements from NIST SP 800-37 Revision 1

Acknowledgements

This publication was developed by the *Joint Task Force Transformation Initiative* Interagency Working Group with representatives from the Civil, Defense, and Intelligence Communities in an ongoing effort to produce a unified information security framework for the federal government. The Project Leader, Ron Ross, from the National Institute of Standards and Technology, wishes to acknowledge and thank the senior leadership team from the U.S. Departments of Commerce and Defense, the Office of the Director of National Intelligence, the Committee on National Security Systems, and the members of the interagency working group whose dedicated efforts contributed significantly to the publication. The senior leadership team, working group members, and their organizational affiliations include:

U.S. Department of Defense

Cheryl J. Roby
Acting Assistant Secretary of Defense for Networks and Information Integration/ DoD Chief Information Officer

Gus Guissanie
Acting Deputy Assistant Secretary of Defense for Cyber, Identity, and Information Assurance

Dominic Cussatt
Senior Policy Advisor

Office of the Director of National Intelligence

Honorable Priscilla Guthrie
Intelligence Community Chief Information Officer

Sherrill Nicely
Deputy Intelligence Community Chief Information Officer

Mark J. Morrison
Deputy Associate Director of National Intelligence for IC Information Assurance

Roger Caslow
Lead, C&A Transformation

National Institute of Standards and Technology

Cita M. Furlani
Director, Information Technology Laboratory

William C. Barker
Chief, Computer Security Division

Ron Ross
FISMA Implementation Project Leader

Committee on National Security Systems

Cheryl J. Roby
Acting Chair, Committee on National Security Systems

Eustace D. King
CNSS Subcommittee Co-Chair (DoD)

William Hunteman
CNSS Subcommittee Co-Chair (DoE)

Joint Task Force Transformation Initiative Interagency Working Group

Ron Ross *NIST, JTF Leader*	Gary Stoneburner *Johns Hopkins APL*	Dominic Cussatt *Department of Defense*	Kelley Dempsey *NIST*
Marianne Swanson *NIST*	Jennifer Fabius Greene *MITRE Corporation*	Dorian Pappas *National Security Agency*	Arnold Johnson *NIST*
Stuart Katzke *Booz Allen Hamilton*	Peter Williams *Booz Allen Hamilton*	Peter Gouldmann *Department of State*	Christian Enloe *NIST*

In addition to the above acknowledgments, a special note of thanks goes to Peggy Himes and Elizabeth Lennon for their superb technical editing and administrative support. The authors also wish to recognize Beckie Bolton, Marshall Abrams, John Gilligan, Richard Graubart, Esten Porter, Karen Quigg, George Rogers, John Streufert, and Glenda Turner for their exceptional contributions in helping to improve the content of the publication. And finally, the authors gratefully acknowledge and appreciate the significant contributions from individuals and organizations in the public and private sectors, nationally and internationally, whose thoughtful and constructive comments improved the overall quality and usefulness of this publication.