Written statement of
W. Wyatt Starnes
Founder, President and CEO SignaCert, Inc.
Before the
House Sub-committee on Technology and Innovation
under the
House Committee on Science and Technology
October 22, 2009

Good afternoon Mr. Chairman and respected members of the Committee. I appreciate the opportunity to present before this committee today.

My name is Wyatt Starnes, a Founder of SignaCert, Inc. and Tripwire, Inc. and currently the CEO and President of SignaCert. Please see my narrative biography for more details on my background and experience.

I should note for the record that I did serve as member of the National Institute of Standards and Technology (NIST) Visiting Committee on Advanced Technology (VCAT), and while I have some recent experience with NIST and the Information Technology Labs (ITL), I am no longer serving as a VCAT member.

As you are aware Mr. Chairman, I have been working closely with both the commercial and government sectors in the areas of information assurance and cyber security for many years. For the purposes of this testimony I will generally reference the Information Assurance and Cybersecurity issues as "Cyber Assurance" for the following reasons:

> In my opinion labeling our challenge as "Cybersecurity" is limiting. Our full goal must be to address ALL issues that relate to improving the security, availability, stability and reliability of the computing devices used to create and deliver complex IT business processes.
>
> We must address the risks that are hostile in source and nature (malicious), as well as hardware and software design, delivery, and maintenance weaknesses (non-malicious) that are also known to induce risk.
>
> It is well established that undetected non-malicious changes do increase malicious risk, and also cause IT business service delivery instability and failure.

It is my belief that we are at a very critical time in our nation's history with regards to our Cyber Assurance practices. We must act now, and bring increased creativity, technology and innovation to these challenges.

I would like to commend this sub-committee, led by Congressman Wu and his staff, for continuing to direct focus to our cyber assurance challenges, and the important contributions that NIST has made, and continues to make, in support of these critical national cyber assurance priorities.

Specific questions posed by the Sub-Committee

The committee posed three questions for me to address during this hearing:

1. What could NIST do to address the recommendations in the 60-day review?
2. What are my thoughts and comments on the Reorganization of ITL?
3. Given the current emphasis on Information Assurance and Cybersecurity, what are my recommendations on how ITL might improve its effectiveness or expand its scope/activities and impact?

NIST and the 60-Day Review

Relative to question one, regarding NIST and the *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (the 60-day review), my personal experience tells me that NIST is already ahead of the curve with its contributions to the key issues and priorities presented in the 60-day review document that was delivered to the President.

Before I address these specifically, I would like to briefly comment on the role of NIST and its legislated mission and budgeted charter.

As the committee knows, NIST is a non-regulatory agency founded on March 3, 1901, as the National Bureau of Standards and was the federal government's first physical science research laboratory.

While it may surprise many citizens, it is no accident that NIST was created as an agency within the Department of Commerce where its primary mission is to ***promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life***.

An even simpler way to state this mission is ***to reduce the friction of commerce by advancing measurement science, standards and technology.***

NIST's role against the 60-day review is clearly in relation to creating and administering IT measurement standards, technology and methods to enable better, and more standardized methods for optimizing the efficacy of cyber assurance methods.

For the purposes of this, my written statement, I would like to elaborate on some of the specific work accomplished by NIST. While there is much more Information Technology Labs (ITL) work that deserves acknowledgment, I will focus these comments on the following areas:

- The 800-series Information Technology Support for Federal Information Security Management Act (FISMA).
- The National Software Reference Library (NSRL) work, and it relationship to the Help America Vote Act (HAVA), and its potential contributions to FISMA and the Security, Content and Automation Protocol (S-CAP).
- The multilateral (public and private) effort to establish and enhance the S-CAP method.

FISMA and the "800-Series" body of work:

From the NIST special publication 800-53 Revision 2 (The bold text was added by this author for emphasis):

> The **Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure**. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. **ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.** The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

With the charter and intent of the work described here (from the same publication):

> This document has been developed by the **National Institute of Standards and Technology (NIST) to further its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, P.L. 107-347. NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems.** This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.
>
> This guideline has been prepared for use by federal agencies. It may also be used by nongovernmental organizations on a voluntary basis and is not subject to copyright. (Attribution would be appreciated by NIST.) Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official.

Mr. Starnes Observations on the 800-series work:

While the creators and authors of the 800-series publications have been consistently humble relative to their contributions in bringing this important work forward, the impact to both government and industry has been enormous.

I congratulate the dedicated teams across NIST for their work and I'd like to specifically commend the director of ITL, Cita Furlani, for her steadfast vision and support of the implementation of this work by NIST ITL in order to serve these critical national needs.

Additionally I would like to recognize Ron Ross, Stu Katzke, Arnold Johnson, Marianne Swanson, Gary Stoneburner and George Rogers and many others for their contributions to this foundational body of work.

Areas for NIST improvement:

In general, the areas I outline below are already well underway by NIST, and I raise them to encourage continued focus only:

- Make the 800-series documents and recommendations easier to read and use by the targeted constituencies. Bigger, in terms of content volume, is not necessarily better. I support the effort to streamline the 800-series documents making them more concise and easier to utilize.
- Continue to drive emphasis with all Federal IT practices, including FISMA and the supporting standards and methods, from "Certification and Accreditation" (C&A) and periodic compliance to "Continuous Monitoring".

Help America Vote Act (HAVA) and the National Software Reference Library (NSRL):

From the NIST website:

The Help America Vote Act:

The Help America Vote Act (HAVA) of 2002 (Public Law 107-252) was passed by Congress "to establish a program to provide funds to States to replace punch card voting systems, to establish the U.S. Election Assistance Commission (EAC) to assist in the administration of Federal elections and to otherwise provide assistance with the administration of certain Federal election laws and programs, to establish minimum election administration standards for States and units of local government with responsibility for the administration of Federal elections, and for other purposes."

NIST's roles under HAVA:

HAVA established the Technical Guidelines Development Committee (TGDC) to assist the EAC with the development of voluntary voting system guidelines. HAVA directs the Director of the National Institute of Standards and Technology (NIST) to chair the TGDC and to provide technical support to the TGDC in the development of these voluntary guidelines.

In addition HAVA directs NIST to conduct an evaluation of independent non-Federal laboratories to carry out the testing of voting systems and to submit recommendations of qualified laboratories to the EAC for accreditation. HAVA also charges NIST with monitoring and reviewing laboratories accredited by the EAC.

National Software Reference Library:

From the NIST website:

This project is supported by the U.S. Department of Justice's National Institute of Justice (NIJ), federal, state, and local law enforcement, and the National Institute of Standards and Technology (NIST) to promote efficient and effective use of computer technology in the investigation of crimes involving computers. Numerous other sponsoring organizations from law enforcement, government, and industry are providing resources to accomplish these goals, in particular the FBI who provided the major impetus for creating the NSRL out of their ACES program.

The National Software Reference Library (NSRL) is designed to collect software from various sources and incorporate file profiles computed from this software into a Reference Data Set (RDS) of information. The RDS can be used by law enforcement, government, and industry organizations to review files on a computer by matching file profiles in the RDS. This will help alleviate much of the effort involved in determining which files are important as evidence on computers or file systems that have been seized as part of criminal investigations.

The RDS is a collection of digital signatures of **known**, **traceable software applications**. There are application hash values in the hash set which may be considered malicious, i.e. steganography tools and hacking scripts. **There are no hash values of illicit data, i.e. child abuse images**

Mr. Starnes' Observations on HAVA and NSRL:

In my opinion, HAVA comprises some of the most important technical work underway by USG to automate and enforce technical and social trust that helps enable our democratic process. HAVA can and should serve as a lighthouse for other countries to follow for enabling a seamless, automated and trusted voting and vote aggregation system.

I note HAVA in my testimony because the methods and technologies specified under the guidance, and the software measurement methods developed under the NSRL programs, have tremendous importance and utility over and above the HAVA use cases.

Essentially HAVA and NSRL represent a practical instantiation of a "trust-based" compute model. I believe that trust-based computing methods are crucial to achieve better and more transparent, holistic Cyber Assurance for both the government and commercial sectors.

A major tenet of the HAVA/NSRL method is the "positive system attestation" methods required by the HAVA language. Under HAVA, Software used to operate electronic voting apparatus must be cryptographically measured and validated to a trusted reference. NSRL data is used to create the "trust reference" for software attestation.

Generally referred to as software "Whitelisting" by industry, these capabilities promise to "close the blind spot" in our view of IT by establishing the capability to ensure the "as-deployed" software state (and ONLY the as-deployed software state) is currently in place on the IT device or system.

This "positive trust-based method" has broad ramifications for government and industry. By fully utilizing whitelisting techniques we can:

- Reduce the exposure of malicious and hostile software that is "hiding in plain sight"
- Establish and prove supply chain validity (provenance) of the software that is deployed on our mission critical IT devices ranging from Servers to Blackberry's. This is increasingly important in the "outsourced" and "open source" world that we now rely on.
- Increase the transparency and automation of complex IT system management by creating a systematic "closed-loop" measure/validate method. This addresses both malicious and non-malicious change quickly and efficiently.
- Enabling continuous monitoring of the positive state of the software stack has been shown to dramatically increase IT uptime and stability, while reducing the labor and manpower required for the delivery of that capacity.

Mr. Starnes' Recommendations to NIST on Whitelisting:

- NIST should explore its role with industry (companies and standards groups) relating to whitelist content exchange standards (XML schemas, etc.) in order to ensure that industry and government content and methods are "interchangeable". This not only serves government customers with improved frameworks such as S-CAP (discussed below), but it also enables industry to better serve broader government initiatives, such as HAVA and other extended NSRL-like use cases, such as improved cyber forensics.
- NIST should encourage industry (especially platform and software vendors) to support supply chain validation methods, such as whitelisting methods and content, as a standard practice for IT systems management and security. Broader adoption and support of Common Platform Enumeration, or CPE, should also be stressed as a part of the software measurement for operational monitoring and supply chain assurance purposes.

<u>The Security, Content and Automation Protocol effort:</u>

The S-CAP (or SCAP) method is described below.

From the NIST website:

> "The Security Content Automation Protocol (SCAP) is a synthesis of interoperable specifications derived from community ideas. Community participation is a great strength for SCAP, because the security automation community ensures the broadest possible range of use cases is reflected in SCAP functionality. This Web site is provided to support continued community involvement. From this site, you will find information about both existing SCAP specifications and emerging specifications relevant to NIST's security automation agenda. You are invited to participate, whether monitoring community dialog or leading more substantive activities like specification authorship.
>
> NIST's security automation agenda is broader than the vulnerability management application of modern day SCAP. Many different security activities and disciplines can benefit from standardized expression and reporting. We envision further expansion in compliance, remediation, and network monitoring, and encourage your contribution relative to these and additional disciplines. NIST is also working on this expansion plan, so please communicate with the SCAP Team early and often to ensure proper coordination of efforts."

Mr. Starnes' Observations on SCAP:

A major goal with SCAP was to create a normalized "content" view, specifically around IT vulnerability and configuration intelligence. Using several databases, vulnerabilities and configurations can be mapped to government IT platforms. This helps serve prescriptive IT device provisioning and deployment, operational compliance, continuous monitoring and remediation.

SCAP provides a powerful and extensible set of methods, content and embedded IT best practices, enhancing system visibility while improving the validation periodicity for complex IT environments.

SCAP is the culmination of many years of public-private cooperation and, within government, one of the best examples of multilateral government -to-government cooperation this witness has seen.

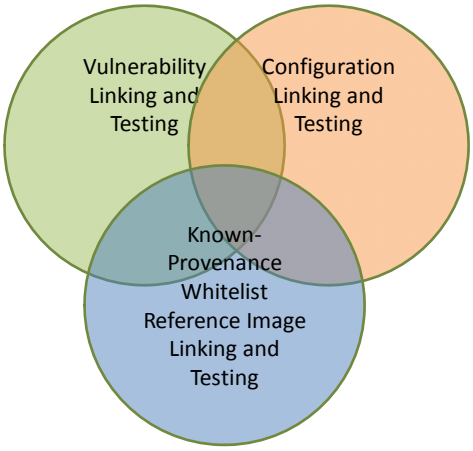
I applaud the efforts of NIST, NSA, DHS, DISA, MITRE and many others for bringing this groundbreaking best practices and content method to fruition.

Industry is already working to extend SCAP methods in several ways including known-provenance image management, as shown within the blue circle below.

Operation Compliance and Readiness

Changing requirements for SCAP

A Leapfrog in Methods



Mr. Starnes' Recommendations on SCAP:

Government IT professionals, including NIST staff and management, are demonstrating pervasive IT leadership with the SCAP methods. It is my belief that these methods will become "de facto standard" not only for Civilian Agencies and DoD, but potentially within the commercial sector.

Vendor support and momentum of the Federal SCAP initiative is growing rapidly and is already impacting commercial companies on both the supplier and end-user side. Most of the major information security companies have, or are readying, SCAP-compliant products for use by their customers.

Additionally, ISV's are adding SCAP protocol to their software measurement content, such as the Common Platform Enumeration (CPE) fields utilized by SCAP.

My personal opinion is that SCAP represents ***the most significant and impactful IT standard, content delivery and best practice framework ever conceived and delivered by the government IT community.***

Again I applaud the NIST team, and broader Federal IT community, for their strong leadership role to conceive and deliver SCAP.

General Observations for the Committee:

We must begin to better focus our IT legislation targeting the specific results that we want the constituencies to deliver. I favor emphasis on the use more carrots versus bigger sticks. It is important to recognize the leadership that led to the creation of important methods such as SCAP. We must also reward the political-will of the departments and agencies that are voluntarily stepping up to implement these important new methods ahead of any regulatory requirement to adopt.

Rethinking our budgeting and regulatory processes to drive faster real results:

With FISMA, government has traditionally focused on Certification and Accreditation (C&A) and periodic compliance checks for agency IT systems and infrastructure. This has resulted in a "check list" mentality where getting a "better grade" becomes the focus. This does not necessarily yield a more secure and robust IT environment.

Additionally, literally millions of dollars and thousands of man hours are spent by government every year to fill three-ring binders that are immediately out of date and irrelevant when the C&A process has been completed. This is driving a false sense of security and is wastes tremendous capital and consumes precious manpower without significantly improving our real cyber risk.

We MUST move to systematic and continuous monitoring solutions that address and adapt to the current realities and dynamic demands of today's cyber world.

Our risk profile now mandates that we move to a more complete "sensor" view (whitelist plus blacklist), along with the active and systematic vulnerability and configuration checking enabled by the SCAP framework. We must change our C&A and compliance mindset, to one of "We are always exposed, so we must continually monitor report and act. This is just common sense.

I urge our legislators in both the House and the Senate to observe and support the tremendous technical work being done by government in partnership with the commercial sector with the SCAP framework.

We (industry and government) are already working side-by-side on live deployments where broad near real-time continuous monitoring is the goal. We believe that these goals are immediately feasible and expect they will quickly prove dramatic improvements in our IT operational readiness.

There is significant and immediate leverage to be gained by shifting dollars allocated for FISMA-based C&A and compliance projects to **full-scope continuous monitoring using the SCAP framework**. I strongly recommend to this committee, and other committees involved in oversight and legislation for targeting improved cyber assurance and regulation, to consider these suggestions.

If we do this (with the close cooperation of the legislative branches, EOP/OMB and DoD), significant National cyber assurance progress can be realized without significant incremental budget impact.

Realigning IT budgeting and spending to our current challenges, and moving from pure C&A to SCAP-enabled Continuous Monitoring, is likely budget neutral to positive. Further, it is expected that the immediate automation advantage will ***lower*** the demand for qualified IT personnel and ***reduce*** long-term IT operational expense.

Reorganization of ITL

On this point I can be quite brief. It is curious to me that an internal reorganization, conducted by the capable and professional management staff of NIST, should draw as much attention as it has. While I am not privy to the precise catalysts of, and motivations for, the contemplated and/or actual organizational event, it seems like the benefit of any doubt should be yielded to the Acting Director and staff at NIST.

That being said, like most organizations – government or otherwise – I would expect that the intent of the reorganization was to realign the human resources with the changing mission requirements. In this case I would further expect that NIST has realized that CYBER ASSURANCE methods and best practices are increasingly a horizontal-cross agency issue, and its core-competencies should not remain in a silo within NIST.

If this is the case, I applaud NIST for adjusting to changing needs, and my only advice perhaps would be a bit more advance marketing and communication to affected NIST constituencies.

Recommendations on how ITL might improve its effectiveness or expand its scope/activities and impact in Information Assurance and Cyber Security

Having worked with NIST from several perspectives for nearly a decade, I have only the deepest appreciation for the dedicated scientists and staff at NIST. I often use the story with family and friends to explain the reach and impact of NIST in the physical world by using the following statement:

In any room, in nearly any country, in any sector of our commercial endeavor - look around that room and I can almost assure you that at least SOMETHING in the environment has been touched, driven or impacted by work done at NIST.

Now when I look from my day-job perspective – and take that same view from a cyber assurance point of view and ask "What impact has NIST had on the security, reliability, stability, and utility of the operational computing infrastructure?"…..We still have work to do.

I encourage NIST, perhaps with even a greater sense of urgency, to continue with its core mission of standards and best practices as they relate to the broader cyber assurance goals and objective.

I further encourage NIST and its government partners in these areas including NSA, DISA, DHS and others, to embrace more "out of the box" thinking around the cyber assurance challenges that the Nation is facing.

TIME IS OF THE ESSENCE:

Mr. Richard Marshall, senior information assurance representative for the Office of Legislative Affairs at the National Security Agency (NSA) said at a public event recently, “We're polishing stones instead of creating stones," he said. "If we don't do something in the near term, there won't be a long term. We are running out of time." I agree.

I encourage NIST to consider the following actions:

- Continue to create and advance measurement standards and methods for Cyberspace.
    - We must do this by continuing to improve our NEGATIVE AND DEFENSIVE posture:
        - This is the Risk and Vulnerability perspective – are we effectively identifying the “Bad things and risky things” in our computer environment – and improving the common language to express and communicate these risks.
        - NIST has done some great work in these areas including the Common Vulnerability Scoring System (CVSS) and National Vulnerability Database (NVD).
        - We need to continue to emphasize these as OPERATIONAL METHODS as opposed to (only) Certification and Accreditation (C&A) and compliance methods.
    - We need to supplement these negative detection and enforcement methods with an improved POSITIVE POSTURE: This is where the prescribed “good state” perspective is captured and enforced. We need operational methods and standards that measure “the known and good state” to assure that our deployed computer environments are intact. We can also address important supply chain provenance issues with these same techniques.
        - NIST has already worked in these areas but they appear “less connected” with the some of the methods described above. Much of this work is apparent in the National Software Reference Library (NSRL) and the Help America Vote Act (HAVA).
        - Many of the same “positive attestation” and trust attestation controls required by HAVA can and should be applied to SCAP-enabled IT operational best practices.

In my view there are MANY parallels between the ways NIST has contributed to this in the physical world for the last 108 years. Software, software assemblies and indeed entire software “stacks” used to enable and enhance our way of life, can and should be measured and operationally attested.

I urge NIST to continue to work multilaterally with their peers in government and industry on all the methods I mentioned above, and to distill these “best of the best” ideas into NIST standards and methods on an even a faster cycle than normal.

Summary

We are a crucial time in our history on multiple fronts. While I fully acknowledge that we are a vendor of methods used to improved cyber assurance, my primary motivation to "join the team" around SCAP and other important developments has been citizen-centered.

We are in a race of dramatic proportions and potential risk, and we are behind. Our National and Economic Security are at risk and if we can improve this as a team, then we must take action now.

We must advance the state-of-the art in Cyber Assurance in order to get to the next level of visibility, control and efficiencies. Extended SCAP methods, along with Continuous Monitoring, are our best chance of getting ahead of our adversaries, and scaling that advantage quickly and efficiently across the Federal enterprise.

I respectfully submit that our technical teams have given us the tools to significantly raise our odds of closing the large cyber assurance gap we now face. It is imperative that our legislative and executive branches show the political-will, and the program and financial resources to enable us to succeed.

Thank you and I welcome any questions from the committee.