Towards Increasing the IT Security Capacity of the Workforce in the United States Intergovernmental System

Report CSPRI-2006-01

Cyber Security Policy and Research Institute
School of Engineering and Applied Science
The George Washington University

January 2006

Lance J. Hoffman
Costis Toregas

This work was supported by a grant from the National Science Foundation.

I. Executive Summary

On October 28, 2005, a small group of experts in computer security and public administration (see Section VII) were brought together to discuss ways that the National Science Foundation (NSF[1]) Scholarship for Service (SFS) program could be strengthened by considering models of collaboration with other governmental levels. These experts explored the design and conduct of a future workshop on the security of government Information Technology (IT) systems that would produce recommendations to leverage existing federal computer security and information assurance (CSIA) education efforts for the benefit of state and local governments.

IT security at the federal level depends not only on federal assets, but also on the capacity of state and local government IT professionals to understand, interface with and support federal efforts. Without a strong capacity in all three levels, interconnected IT systems are vulnerable to errors made by omission or commission at the weakest link. It is not optimum to fund development of cybersecurity specialists at the Federal level for work only in the Federal government if state and local government systems (which are often interconnected to Federal systems) are weak due to design flaws or to lack of appropriately trained personnel to operate them.

The NSF SFS program is a successful effort to promote information security skills in the academic world and to persuade students to consider a career in the public sector. Currently, students in the SFS program graduate and go on to jobs at the federal level. However, concentration of talent within one tier of our intergovernmental system may not produce a strong national (as opposed to federal) IT security environment, and misses an opportunity to bring additional security assets to the entire system. Additionally, the system of training and education currently does not ensure that employees at all three levels of government share the protocols and strategies that can form a hardened and secure infrastructure.

The Planning Meeting participants also were cognizant that the vast majority of IT infrastructure lies in the hands of the private sector, and felt that any long term, lasting solution must also engage and involve leaders from the private sector as well. This has been recognized elsewhere, for example in energy security and the successful national Y2K effort.

The Planning Meeting participants recommend a combined governmental strategy meeting of all three tiers of government that would explore an effective way to leverage federal investments through state and local participation in IA. In order to prepare for this, federal, state and local leaders would be first assembled in small sectoral sessions that would establish a common vocabulary and syntax for IT security in the intergovernmental domain, identify the barriers

[1] Abbreviations are defined in Section VI.

and incentives for intergovernmental action, and finally identify a set of practical actions that could be accomplished. Once the outcomes of these sectoral meetings are documented and synthesized, an integrated meeting of representatives from all three levels of government would discuss the opportunities and barriers to collaboration and produce action items for consideration and implementation by the SFS program and by others.

II. Current Situation and Future Potential

University SFS programs

Since the beginning of the SFS program in 2001, over 300 students have been placed in CSIA-related federal government jobs. While originally most students entering the SFS program had purely technical backgrounds and interest, recently the SFS students' profile has been broadening and the program is seeing more student majors in public policy, business administration, and other relatively less technical fields. More aggressive matching of students with other opportunities (embodied in the January 2005 and 2006 job fairs sponsored by SFS in Washington) are resulting in a broader dispersion of these graduates across the Federal government than in a few very technically oriented agencies. This provides an opportunity to build a broader foundation of support for an intergovernmental approach to IT security. The students now being trained may represent a variety of interests beyond the federal agency level and may be able to work well with state and local officials to solve shared problems and address mutual issues.

While no statutory restriction appears to exist on use of SFS funding in other levels of government, there are political and other barriers. For example, some entities are reluctant to accept federal funding which may develop budgetary pressures in future years should the funding be curtailed or terminated.

It is important to keep in mind that university programs are not the same as certification programs such as those associated with SANS (www.sans.org), ITAA (www.itaa.org), and CISSP (www.cissp.com); these do training, which is more narrow than academic education. However, many state and local governments will use certification as a qualifier for new hires, so an understanding of the driving forces behind program development, funding and trainee attraction is important to the effective design of a national (as opposed to federal) IT security program.

Internship programs

A key mechanism that creates interest and provides linkage to future employment is an attractive and effective internship program. Good examples of such summer internship programs are the ones run by

GAO (http://www.gao.gov/jobopp.htm),
CBO (http://www.cbo.gov/employment/intern.shtml), and the SURF program(s) at NIST (www.surf.nist.gov) and elsewhere. These appear to work well and appear early with specific offers in the lives of students, which make them effective and popular. Replication of key aspects of these programs would be a great help in any subsequent SFS program modification that increases the ability of state and local governments to deal with CSIA issues.

State and local governments hiring

State and local governments (especially small, rural and frontier jurisdictions) mine their own people for jobs; sometimes they are the only people available. Small states often cannot afford a CISO, and can't pay national going rates for technology expertise. Thus, they cannot compete with federal agencies as an employer of choice. If the weakest link determines the strength of any given chain, a national IA program must think of ways to mitigate this problem and create positive incentives for employment in these smaller work places. Sharing of expertise or experts themselves under some sort of sharing arrangement or Intergovernmental Personnel Act (IPA) framework could also mitigate the negative effects of the geographic and financial difficulty which today weakens government CSIA at a national level.

There is also a great deal of experience that has been assembled and used within the federal establishment. We can take what we know from this federal side and export it to the state and local levels. For example, a small subset of PIs from the SFS program at the federal level could be brought together and asked to consider changes and programs that could replicate their experiences at State and Local levels. The mechanism for the successful "exporting" must include an understanding of the different cultures that prevail at the state and local levels, and an adaptation of federal strategies and programs to this different environment that provides employees the opportunities and challenges of being very close to the citizen and the service delivery point.

The use of federal experiences at the state and local level is seen in a variety of fields already. A good parallel example of successful partnership in another program area is the law enforcement community, where the common and agreed need for interoperability is driving federal dollar availability for equipment and the creation of standards and common protocols simply as a way to satisfy funding criteria. When funds are made available for the procurement of hardware, software or services in the public safety arena, they are often accompanied by strict requirements for interoperability with existing federal IT platforms. While state and local people have the flexibility to choose vendors and systems most appropriate for their local conditions, the interface requirements to federal systems become essentially a major driver and discriminator in the selection process. In this way, the intergovernmental funding system becomes a

mechanism to also align IT systems and protocols between the federal, state and local levels.

In order to convince these other levels of government of the importance of focusing on people and programs in the IA arena, it is vital to appreciate what motivates them to recognize and assign scarce resources to any given issue. If senior officials such as a governor or a high visibility county executive are to be attracted to these discussions, the notion of IA would have to be attached to important, policy-intensive issues that can truly attract and hold the attention of policy makers, such as the sustainability of business and state revenues.

Institutions that can take the SFS program nationally to the state and local governments community including Washington-based organizations like NACO (for all counties), NASCIO (state CIOs), NLC (all cities) and PTI (city and county technology leaders) give pathways to large numbers of officials and can be involved in the early stages of program design. Their ability to create an interest around national issues through magazine and website articles, conference presentations, brochures, and other communication vehicles can be harnessed to good use as warranted by program needs.

III. Possible Actions

Current capacity in IT security, while needing improvement at the federal level, is even weaker at the state and local level; it is possible that outreach programs from the Centers of Academic Excellence or other university-based organizations could address this weakness. There are already some models to draw on, but too often these rely on the expertise and energy of one individual, and there is no specific reward or encouragement for most persons in charge of these programs to draw upon these models or to develop their own.

Another possibility to explore is the potential eligibility of state and local IT officials for relevant federal education and training programs. The Scholarship for Service program is a significant resource, but currently only produces workers for the federal workforce. Replication of relevant parts of federal information assurance scholarship programs at state and/or local levels, mechanisms that could allow graduates of existing federal programs to work more effectively with State and local governments, and other possibilities of multiplying the effects of these programs will be helpful in solving the problem.

Figure 1 illustrates the federal, state and local dialog that can be initiated in order to increase the IT security capacity of the government workforce. It is based initially on the SFS program, but both participants and the sponsor agencies during the October 2005 planning meeting recognized and posited that an effective program should not be bound by the SFS program. Indeed the "Big Picture" goes well beyond the SFS program. As a consequence, this report notes the total problem of IA as endorsed by the participants of the Planning

Meeting, and suggested actions are not bound by the current SFS program and its fiscal resources.

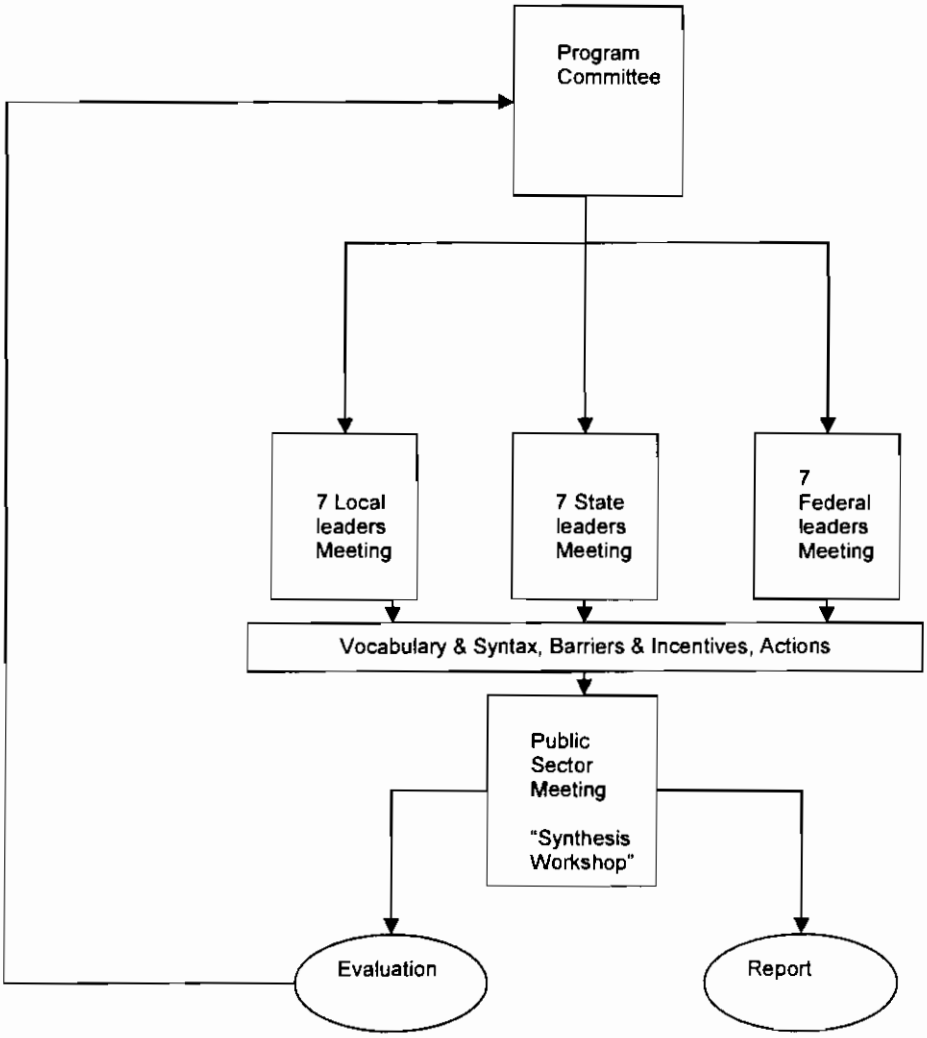

Figure 1
Information Security and the Intergovernmental System- an Opportunity for the SFS program to Use Leveraging Workshops to Enhance CSIA

Such a dialog can best be initiated through the design and execution of a series of leveraging workshops, attended by 7-15 leaders in the field and deployed in hub cities throughout America for easy participation of state and local government officials from all federal regions. The succinct outcome of each Workshop would be to "*increase the IT security capacity of the workforce in the Intergovernmental system*". The next section provides more texture and detail on this proposed series of Workshops and how they may be developed and executed within the first three quarters of 2006.

IV. Details of Proposed Leveraging Workshops

Before the Workshops

1. Foundation Paper

In anticipation of the series of Workshops, a foundation paper will seed the discussion with early thoughts derived from the October 2005 Planning Meeting discussion and other elements, providing a "straw man" to each group being assembled. This paper will have three objectives:

- *Brief description of national cyber-infrastructure*
- *Gross risk analysis of infrastructure, including estimates of the IT security impact on business costs and business continuity. This would provide a clear statement of value for IA (with hard data on skills missing etc)*
- *Posit a series of actions to be taken in unison by the various levels of government which would strengthen IA at all levels.*

2. Reaction papers by participants

The "ticket of admission" to the workshop should be a short written document that describes how the writer would be affected if some of the ideas in the foundation paper (distributed in advance) come to pass. It should also point out what is missing from the current thinking as articulated in that paper. This reaction paper can be as short as one page or as long as desired; indeed, in workshop planning, a slot or two may be reserved for "exceptionally relevant" presentations to be expanded upon. The collection of these early papers could be circulated in advance of the workshop to all participants so there would be recognition of the intellectual capital and ideas present in the room before the meeting begins.

At the Workshops

The program itself would be similar for each of the three tiers of government. It would first identify and catalog a "vocabulary and syntax" of IA, by ensuring a semantically consistent series of terms by which different people describe the same event, and organize reaction to threats in clusters of similar strategies. It would then help the participants see more clearly the series of barriers and incentives that can be recognized and quantified, and finally it would build a series of potential actions that would strengthen the capacity of those employed in the intergovernmental system to secure the IT infrastructure of the nation.

Beyond the educational program, an important element for each workshop would be the human networking and the establishment of understanding of the different cultures and resources available at each level of government. Both formal and informal networks are vital to be established in each level of government around IA and the role of student training and education, and the connections created could become extremely valuable in the event of real disasters or challenges in the future.

The effort to refine the possible action items may include ways to leverage the existing SFS program, the design and support of scholarship programs for new recipients, the creation of capacity building efforts for new recipients, and/or possible program modifications and expansions that take advantage of state and local flexibilities. Modifying the SFS base to include state and local governments, as well as non-governmental organizations (NGOs) is a potential exploration topic, as is weighing the selection criteria for successful candidates in a way that favors state and local government interaction with the federal government.

Students (both pre-work students and in-service employees doing graduate programs) in Public Administration are another important but currently underutilized resource. The advantage of focusing on such students is that they already appreciate and respect the notion of pubic service, so their buy-in and excitement would be more evident early on. In addition, such an approach may reduce the defection to private industry once the students' 2 year service requirement is met. Many of these students may have to be given some technological education to deal with the basics of a nation and world that is increasingly using Internet-based services.

Finally, a workshop could produce some "outside the box" thinking (such as law enforcement LEAP program, paying for state and local governments employees with federal dollars) that could have a lasting effect on the national infrastructure. Existing partnership programs between national associations may also offer viable models; for example NASPAA and ICMA have created a program to concentrate national level internship information and selection programs; a similar effort could be undertaken in the IA arena, with participants expanded to include NLC, NACo, NGA, NASCIO and multi-state ISACs, in a way which would build national attention to the target audience and make use of the membership

and communications assets of these national associations, thus recognition to and focus on meritorious programs.

Deliverables

Beyond the networking and relationship building between the three tiers of government, the Workshop effort would develop a set of mutually recognized and accepted statements of federal, state and local concerns about IA, organized and synthesized in a similar fashion. In addition, the barriers and incentives to intergovernmental collaboration would be presented, and finally the collective judgment of the experts and practitioners regarding needed action items would be presented in succinct, written form.

A desired outcome of the workshop is also the expansion of the circle of organizations committed to strengthening IT security of the nation and their active integration in the collaborative effort necessary to implement such a national program. It is therefore conceived that action items corresponding to the workshop recommendations would be identified, and attendees might accept responsibility for accomplishing various go-forward tasks. By being able to translate IA requirements to more far-reaching objectives such as economic development, business continuity and homeland security, it is hoped that buy-in will be secured at the personal, as well as the institutional level.

Venue and Timing

The participants of the October 2005 Planning Meeting were insistent on favoring venues outside the Washington DC area so that a good geographic representation can be struck in each of the follow-on workshops. It was also felt that it may be wise to select a symbolic location for the workshops outside of the Washington DC area, and to make sure that the actual hotel chosen for the participants does not give the impression of unwise use of public funds (e.g., a hotel around Chicago's O'Hare or Kansas City's airport hubs or the Claremont hotel in Oakland) so impressions are not of lavish spending and so people from all parts of the nation might see the travel time as acceptable.

A likely time for the workshops is the Spring/Summer of 2006, with April (slack time after hearings before start of fiscal year for those jurisdictions with July budgets) being a preferred month for the state and local participants of the Planning meeting. A timeline for the proposed effort is shown in Figure 2. If the effort is initiated in mid January, 2006, then initial results from all meetings can be seen by late May. If funding is approved for a March 1, 2006 start, then early results would become available by mid July, 2006.

Figure 2. Timeline for Proposed Effort

Week 0	Receipt of NSF approval
+ 1 week	Foundation Paper initiated
+ 2 weeks	Venues reserved
+ 2 weeks	Attendees identified
+ 2 weeks	Speakers identified
+ 4 weeks	Acceptances received
+ 4 weeks	Foundation paper mailed out
+ 6 weeks	Responses and reaction papers received
+ 8 weeks	Federal government-oriented workshop
+ 8 weeks	State government-oriented workshop
+ 8 weeks	Local government-oriented workshop
+ 10 weeks	Synthesis workshop planning
+ 12 weeks	Final invitees selected
+ 12 weeks	Venue selected
+ 12 weeks	Invitations delivered
+ 14 weeks	Synthesis workshop conducted
+ 16 weeks	Final report delivered

Funding

There are three layers of federal resources that could be mobilized to organize this IA effort: within the SFS program, NSF-wide, and on an inter-agency basis which goes outside the NSF organizational and funding schema. Since the federal workforce is not the only workforce that is protecting the federal infrastructure, NSF may want to consider partnerships with other agencies and other levels of government that have responsibility in this area, such as DHS, to organize funding efforts as well.

A solid funding strategy would not only enable the development and execution of a series of workshops, but might point the way towards funding innovative intergovernmental pilot programs or exchanges of proven successes from one governmental level to another. This current stage of brainstorming could also result in "outside the box" dialog and recommendations which may suggest federal strategies which today simply cannot be contemplated because of programmatic inertia or lack of resources. It is possible, for example, that an effort to create and fund a CISO position in each and every state of the union could have a salutary and significant effect on federal program and data security by strengthening the state level defenses in the IA arena. Such dollar expenditures that would support non-federal governmental training and education at the state and local level could in fact improve the federal IA performance by hardening the national IT security capacity. Indeed, it is even possible that funds for such a state-by-state program could be found at the state level through their

own departments of Education or Technology training, either on a matching basis or as stand alone funds. Such a leveraging effect of federal dollars and such a direct and discernible benefit to each and every state of the Union could have a helpful effect on legislative attitudes and support for the program.

V. Considering the private sector

The Planning Meeting participants also were cognizant that the vast majority of IT infrastructure lies in the hands of the private sector, so any long term, lasting solution must engage and involve leaders from the private sector as well. Thus, a multi-phase, parallel strategy was recommended which could structure the energies and interest of pubic and private sectors in creating a secure infrastructure and organize practical ways to accomplish this in the context of the SFS program and beyond.

As Figure 3 suggests, the previously described series of governmental employee meetings (funded by the NSF [encompassed by the dashed border in the figure]) could be mirrored by similar industry leader meetings (perhaps funded by the DHS). There are in place several ISACs (Information Sharing and Analysis Centers) in each of the major industry groupings, and they could form a quick and strong link to the overall private sector strategies in IA. A combined meeting of the best participants from each stakeholder community could drive outcomes useful to the "big picture" concerns so important to the nation's IT security. Such a multi-phase, parallel strategy would structure the energies and interest of pubic and private sectors in creating a strategy towards a more secure national infrastructure and organize practical ways to accomplish this in the context of the SFS program and beyond.

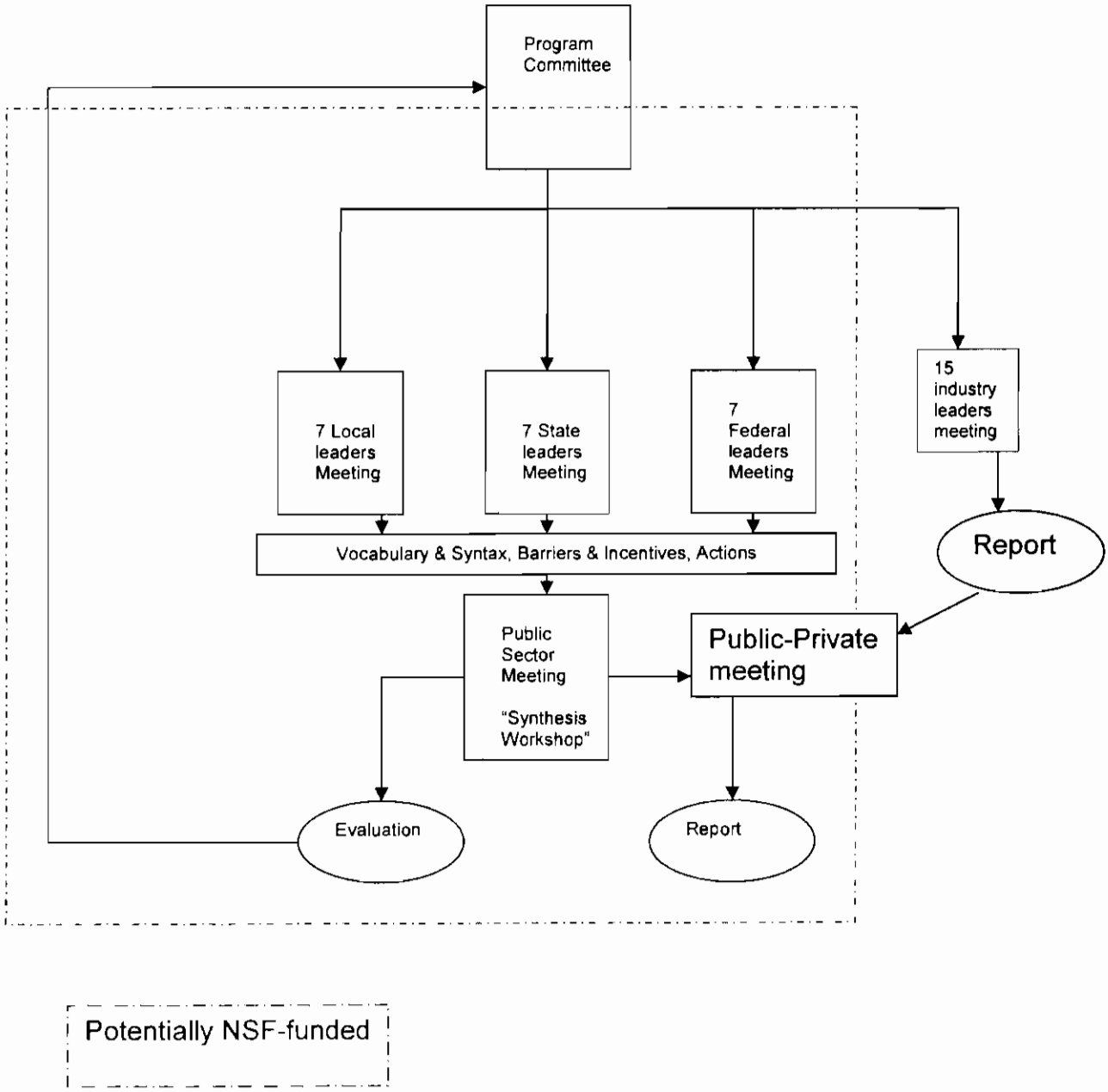

Figure 3.
Information Security at National Level - a Potential Schema for Public/Private Collaboration

VI. Abbreviations used:

CBO	Congressional Budget Office
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CISSP	Certified Information Systems Security Professional
DHS	Department of Homeland Security
GAO	Government Accountability Office
IA	Information Assurance
ICMA	International City and County Management Association
ISAC	Information Sharing and Analysis Center
ITAA	Information Technology Association of America
LEAP	Law Enforcement Assistance Program
NACo	National Association of Counties
NASCIO	National Association of State Chief Information Officers
NASPAA	National Association of Schools of Public Affairs and Administration
NGA	National Governors Association
NIST	National Institute of Standards and Technology
NLC	National League of Cities
NSA	National Security Agency
NSF	National Science Foundation
PI	Principal Investigator
PTI	Public Technology Institute
SANS	System Administration, Audit, Network, Security Institute
SURF	Summer Undergraduate Research Fellowship

VII. Planning meeting Attendees

The planning meeting took place on October 28, 2005 at the Mount Vernon campus of The George Washington University. Participants were:

Otto Doll, Chief Information Officer and Commissioner of the Bureau of Information and Telecommunications, State of South Dakota

Diana Gant, Program Director, Scholarships for Service program, National Science Foundation

Ira Hobbs, Chief Information Officer, U. S. Treasury Department

Lance Hoffman, Distinguished Research Professor, Computer Science Department, The George Washington University, Washington, DC

Hun Kim, Deputy Director, Strategic Initiatives, Information Analysis and Infrastructure, U. S. Department of Homeland Security

Dave Molchany, Fairfax County (VA) Chief Information Officer and Deputy County Executive

Kathryn Newcomer, Director, Public Policy and Public Administration Program, The George Washington University

Frank Reeder, Chair, U. S. Information Security and Privacy Advisory Board

Costis Toregas, Lead Research Scientist, Computer Science Department, The George Washington University, Washington, DC