

The Flyzik 5

By Jim Flyzik, The Flyzik Group



Top 5 Programs that Need to be Coordinated with a Cyber Security Program

Cyber Security Programs cross many organizational boundaries and require more than just the efforts of and CIO and CISO offices. Here are 5 "must coordinate" Programs for a good Cyber Security Program. A good Cyber security strategy will include coordination with:

1. Identity Management Programs: Positive identification of people and all devices on the network.
2. Privacy Programs: Tools to protect from loss of both unstructured and structured data and using proxy data for any sensitive information leaving the production environment to prevent disclosure of any information and to assure compliance with Privacy Directives.
3. Human Capital Security Programs: Background Security checks, awareness and education campaigns and holding employees accountable for Cyber Security policy compliance a necessary element of a comprehensive program.
4. Physical Security Programs: Physical security controls designed to minimize risk of unauthorized access to areas containing sensitive information.
5. Records Management/Classification Programs: Cyber Security programs must be consistent with policies for guarding classification of information, records retention and records discovery initiatives.

Jim Flyzik
President, TheFlyzikGroup
Chairman, Information Technology Association of America
Homeland Security Committee
jflyzik@theflyzikgroup.com
(o) 301-365-4772 •(c) 410-262-1236 •(f) 301-365-6385
<http://www.theflyzikgroup.com/>



Thought Leadership

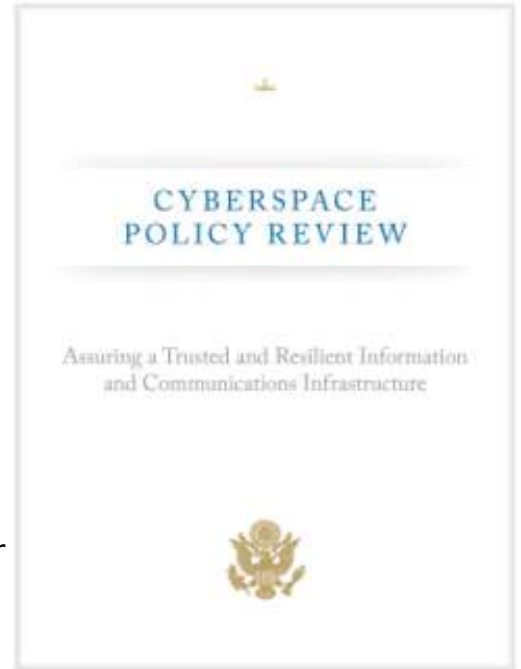
In Understanding Cyber and Homeland Security Issues

by Tom Trezza, Jr.
President, Trezza Media Group

On December 22nd, 2009, President Obama officially selected Howard A. Schmidt, former cyber advisor to President George W. Bush, to be the CyberSecurity Coordinator to orchestrate the government's strategy for protecting computer systems. In May of 2009, President Obama declared the nation's digital networks a "strategic national asset" and said that protecting them would be a "national security priority."



The [CyberSpace National Review](#), which was published in the May 2009 timeframe, outlined 10 Near Term Action Plans, with the top priority of announcing a CyberSecurity Policy Official whose responsibility is to coordinate the Nation's CyberSecurity Policies & Strategies. So Step 1 has been taken and now the questions are: what is Industry's role and how can you help provide Cyber and Homeland Security Solutions to our Federal Government and Nation at large.



Every year, Jim Flyzik & I host our 1st Federal Executive Forum on CyberSecurity in late January & AFCEA International hosts its annual [Homeland Security Conference in February](#) (Feb. 24-25, 2010). Our FEF Program included Mr. Greg Schaffer, Assistant Secretary for CyberSecurity/DHS, Mr. Dave Wennergren, DCIO/OSD & Ms. Priscilla Guthrie, CIO/IC. The Forum gave a great view of what is being done, what is needed and the challenges across the DHS-Defense and Intel Communities. I thought I would outline some key discussion points in order for Industry to continue to build strong partnerships with its government customers.



Federal Executive Forums

CyberSecurity "Progress and Best Practices" February, 2010



This Program discussed:

- Progress Report on CyberSecurity with DHS-DoD & ODNI
- Top CyberSecurity Priorities
- Update on the DoD Cyber Command Initiative
- Key Challenges to still overcome in IT Security
- Lessons Learned
- A Vision for The Future-how can we be proactive and prevent attacks

Panelists:

- Greg Schaffer- Assistant Secretary for CyberSecurity & Communications, DHS
- Dave Wennergren- DCIO, OSD
- Priscilla Guthrie- CIO, ODNI
- Lee Holcomb- Vice President, Strategic Initiatives, Lockheed Martin Information Systems & Global Services
- Robert Dix- Vice President, Government Affairs & Critical Infrastructure Protection, Juniper Networks
- Mike Carpenter- Senior Vice President for Public Sector, McAfee

Moderator: Jim Flyzik -Flyzik Group

To watch the video or listen to the audio on this program,

please click [here](#).

The Government Cloud - "DOD

Understanding CyberSecurity Issues

Below are some of the top priorities and key challenges facing our top government cyber leaders:

Top Priorities:

- Finding the right skilled professionals
- Building key partners in Government & Industry
- Protecting information under stress
- Security Solutions need to be completely different than in the past
- Work more effectively with Mission Partners
- Have Secure Information Sharing

Top Challenges:

- Raising Awareness of the Risk v. Responsibility
- Putting Relationships, Policies & People in Place
- Balancing the Need to Share v. the Need to Secure
- Protecting every Node on every Network
- To Share Information-Globally

This is our 5th year of working closely with top Government IT Leaders and it's always interesting to hear how important their Industry Partners are to meeting their Mission Needs. As outlined in the CyberSecurity Policy Review, the status quo is no longer acceptable, so it's up to leaders in Industry to continue to listen and provide solutions to protect our critical infrastructures and data-which are "strategic national assets."

Understanding Homeland Security Issues

To help solve DHS's mission problems, it's critical to know and learn about the most current Homeland Security issues facing our nation and our fight against terrorism. [The AFCEA Homeland Security Conference](#) (Feb. 24-25, 2010) has always been the Premier Event in Washington DC.

Becky Nolan, Jim Flyzik and their Advisory Board have developed another amazing two day event that will cover all of the major Homeland Security Issues, including:

- Priorities of the New CyberSecurity Coordinator
- DHS CyberSecurity Priorities
- Border Security Programs & Priorities
- Information & Intelligence Sharing Priorities
- DHS CIO Roundtable Discussion (FEF Program)
- DHS Acquisition Reform & Priorities
- Immigration Reform & Priorities
- Emerging Social Media & Transparency Con



The Government Cloud - DOD Progress and Best Practices" November, 2009



This Program Discussed:

- Progress Report on Cloud Computing in Federal Government
- Progress & Best Practices including the DISA RACE Program
- Challenges still ahead including Security
- Lessons Learned
- A Vision for The Future for Cloud Computing

Panelists:

- Robert Carey- CIO, Navy
- Mike Krieger- Army Deputy Chief Information Officer, Office of the Secretary of the Army
- Henry Sienkiewicz- Technical Program Director, Computer Services, Defense Information Systems Agency
- Dr. Ron Ritchey- Partner, Booz Allen Hamilton
- David Smith- Chief Technology Officer, Citrix Systems
- Tim Harder- Business Development, EMC Federal Systems

Moderator: Jim Flyzik -Flyzik Group

To watch the video or listen to the audio on this program, please click [here](#).



- Emerging Social Media & Transparency Gap

To learn and network with DHS Leaders, I would strongly recommend spending these two days listening, learning and understanding the needs and priorities of DHS for 2010 and beyond. These are challenging times in the federal government cyber and homeland security space and we all need to step up and help government solve these mission critical issues.

- Tom

Make It Easier, Bake It In

By Jeff Erlichman, Public Sector Communications



I admit it. I'm one of those "end users" on the frontlines of my personal and business cyber defenses.

When it comes to security, the Cyber Space Review Plan doesn't have to spend its resources telling me. Believe me, I'm aware. You better be--especially when your email is in the cloud.

I've long known and practiced the virtues of proactive cybersecurity and having multiple backups. But it didn't prevent me from being attacked. I have one email account that has taken my provider more than 6 months to figure out the problem. And I'm still not 100% sure it's solved.

If you are like me, here's what you've got. I have a one program that provides a "Security Center" protecting my computer, files and email from viruses, spyware etc.

I have another program that scans, repairs and optimizes my PC. Plus, I have another anti-spyware program. I'm not sure whether these programs actually conflict or are complementary. In fact, I'm confused. I would ask my systems administrator, but of course, that's me. And I don't know the answer.

But I do know one thing: I'm practicing "cyber hygiene". I'm cyber responsible, but still frustrated, still not sure I'm doing enough, and still wishing the whole cybersecurity process was easier and more transparent.

So, I can't tell you how refreshing it was to hear some leading security providers say the industry isn't doing enough to help end users.

HP's Sam Chun has written on security awareness. During our recent Roundtable he said, "I think we on the industry end have made it fundamentally too difficult for the end user to achieve security. I think we as an industry need to do better; it's just too hard and too complex for the average user."

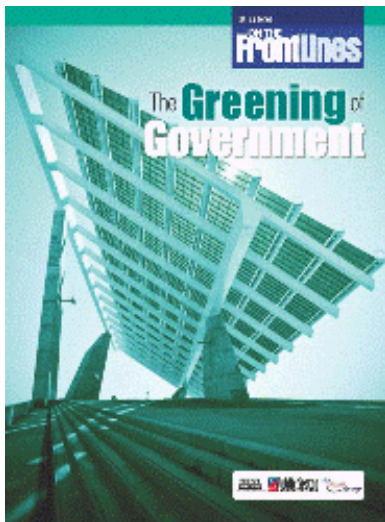
Chun said we need to make security transparent, invisible, assured and persistent for the end user so it is just computing



[Click Here to Reserve March Issue](#)



[Click Here to Download](#)



[Click Here to Download](#)



for them. "The industry needs to work harder to make this happen. We should not expect the user to do it effectively; so we as an industry need to help them do it."

CSC's Sam Visner added "for many years hardware and software manufacturers and SIs said 'we are going to turn IT into a commodity; one that is increasingly available, increasingly useful and increasingly easy to use; so you shouldn't worry about IT'."

But now some are telling end users they haven't done enough. They don't update antivirus definitions or don't figure their firewall right Visner explained. "Everything we told you about IT being inexpensive, easy and useful, now we have a big and difficult discipline that you--the user--have to do. That wasn't the deal when we rolled out IT."

Hallelujah! I'd love to do nothing, but I'm a realist. It may become simpler, but proactive personal cybersecurity is never going away.

But I'd like every cybersecurity provider to have Visner's attitude.

"If we design the system properly, we do not have to expect users to do all the maintenance; if we design it properly, users don't have to become cyber experts; and if we 'bake in' cybersecurity as an intrinsic system component, then IT becomes increasingly available and inexpensive, becomes easier to use and becomes useful to the mission."

That's the attitude I want. Bring it on.

Jeff

Public Sector Communications
19009 Alpenglow Lane
Brookeville, MD 20833
301-774-6660 office • 301-980-8235 mobile • www.PubSector.com



AFCEA Bethesda Chapter's Annual Federal Budget Preview Breakfast February 26th, 2010

On February 1, 2010, President Barack Obama requested \$79.4 billion in spending on information technology projects for fiscal 2011, a 1.2 percent increase from what he proposed in fiscal 2010. Join leaders from three of the largest federal agencies on February 26, 2010 at AFCEA Bethesda Chapter's annual Federal Budget Preview breakfast. Panelists to look at the 2011 IT budget priorities and answer industry's most pressing questions:

• How will next year's budget reflect the president's



[Click Here to Download](#)



Trezza Media Group Capabilities

Trezza Media Group offers a variety of media and marketing services including media planning, custom publishing, custom events, strategic planning, research, on-site government and industry and industry training and media sales representation. TMG has partnered with some of the leading professionals in the government market to provide these services. [Download the brochure here.](#)

- How will next year's budget reflect the president's ongoing agenda in areas like healthcare, education, energy and the environment?
- What will the continuing push towards transparency, reusability of data and cloud computing bring in terms of IT budget priorities?
- What new technology applications should agencies invest in to enable intra-agency and interagency collaboration and create a coordinated process for identifying and implementing social media tools in open government?
- How might the winding down of the war in Iraq and the surge in Afghanistan be reflected in IT budget priorities?

Speakers include:

- Vivek Kundra, Federal Chief Information Officer, & Administrator, Office of E-Gov and Information Technology, Office of Management and Budget (Invited as Moderator)
- Roger Baker, Assistant Secretary for Information Technology & Chief Information Officer, Department of Veterans Affairs
- Vance Hitch, Chief Information Officer, Department of Justice
- Dave Wennergren, Deputy Assistant Secretary of Defense for Information Management, Integration and Technology & Deputy Chief Information Officer, Department of Defense

To register or more information on the program including sponsorship opportunities, please visit www.bethesda-afcea.org/febbreakfast.

[Click to forward this email to a friend!](#) [Click to view this e-mail as a web page.](#)

This e-mail was sent by Trezza Media Group, located at 570 Van Emburgh Avenue, Township of Washington, NJ, 07676 in the USA.

We value you as a client, but if you would prefer to discontinue receiving our newsletters, please click