

## Assured Communications and Information Sharing: Serving the Public, Protecting the Nation

### About the Federal Government Leadership Forum

The Federal Government Leadership Forum (the forum) is a program of executive-level dialogues among private-sector and information technology leaders serving military, civilian, and intelligence agencies of the U.S. government.<sup>1</sup> The purpose of the forum is to facilitate ongoing collaboration among agencies and the private sector to improve our nation's communications in the area of homeland security and defense.

### About this document

ViewPoints is produced by Tapestry Networks and presented to all members of the Federal Government Leadership Forum. Its purpose is to synthesize key issues arising from discussions that took place during the most recent forum meeting and to advance the conversation on information sharing and assured communications as they relate to homeland security. ViewPoints reflects the forum's use of a modified version of the Chatham House Rule whereby names and affiliations of participants are a matter of public record, but comments made during meetings are not attributed to individuals, agencies, or corporations. Recipients of ViewPoints are encouraged to share it freely in the belief that the inclusion of additional public- and private-sector executives in this dialogue will increase the value of the discussion and the security of the nation.

### Participants

The members of the forum participating in the meeting were:

- **Greg Baroni**, Corporate Vice President, President, Global Public Sector, Unisys
- **Lieutenant General Steven Boutelle**, CIO/G-6, U.S. Army
- **Joel Brunson**, Vice President, Federal Sector, Avaya
- **Lieutenant General Charles Croom**, Director, Defense Information Systems Agency
- **Jim Flyzik**, Chairman, Committee on Homeland Security, ITAA
- **John Gilligan**, Vice President & Deputy Director, Defense Sector, SRA International, Inc.
- **Brent Greene**, Vice President, Strategic Initiatives, Lucent Technologies
- **John Grimes**, Nominee - Assistant Secretary of Defense, Networks & Information Integration and CIO, U.S. Department of Defense
- **Vance Hitch**, CIO, U.S. Department of Justice
- **Becky Nolan**, Executive Vice President, AFCEA

---

<sup>1</sup> The forum was initiated by Don Peterson, Chairman and CEO of Avaya, in support of the mutual commitment of the government and the private sector to assure effective communications for homeland security. The forum is sponsored by Avaya and Northrop Grumman and produced by Tapestry Networks in collaboration with the Armed Forces Communications and Electronics Association (AFCEA) International. This document has been prepared by Tapestry Networks in association with the members of the Federal Government Leadership Forum.

- **Don Peterson**, Chairman and CEO, Avaya
- **Tom Shelman**, Vice President, Internal Information Services and CIO, Northrop Grumman
- **Linton Wells**, Acting Assistant Secretary of Defense, Networks & Information Integration and CIO, Department of Defense
- **Dave Zolet**, Vice President, Corporate Business Development, Northrop Grumman

**Guest:**

- **Phil Reiting**, Senior Security Strategist, Microsoft

**Discussion Leaders:**

- **George Goldsmith**, CEO, Tapestry Networks
- **George Anderson**, Executive Producer, Tapestry Networks

**Regrets included:**

- **Vice Admiral Herb Browne**, U.S. Navy (Ret.), President and CEO, AFCEA
- **Linda Gooden**, President, Lockheed Martin Information Technology
- **Lee Holcomb**, Chief Technology Officer, Department of Homeland Security
- **Major General Dale Meyerrose**, U.S. Air Force (Ret.) Nominee – CIO, Office of the Director of National Intelligence
- **Lieutenant General Harry Raduege**, U.S. Air Force (Ret.)
- **Lieutenant General Robert Shea**, Director for Command, Control, Communications, and Computer Systems, Joint Staff J-6
- **La Forrest Williams**, Chief of Information Technology Policy, National Security Agency

**Executive Summary**

The fourth meeting of the Federal Government Leadership Forum took place at the end of a historic hurricane season and a period of increased outreach by the forum to key stakeholders, especially those in the private sector. This combination of circumstance and forum effort lent renewed energy to the forum's work on assured communications and information sharing.

Hurricane Katrina had an extraordinary impact, rendering America's eleventh-largest city uninhabitable. It was also the first event to be categorized a national catastrophe since the post-9/11 creation of the Department of Homeland Security (DHS). Members agreed that Katrina showed above all else the need for both clear command and control and assured communications capability. They were concerned that the lack of clearly defined roles and responsibilities and resulting confusion contributed to a significant leadership gap. In too many cases the void created by that lack of leadership *"was filled by the media."* Members offered this assessment in the spirit of situation analysis and committed to greater collaboration and cooperation with DHS to avoid a reprise of the chaos that followed in Katrina's wake. There was consensus that the lack of access to the communications infrastructure had been foreseen and had to be addressed.

Five months ago, in the spirit of *"cracking the code for really integrating the great ideas into [results that would make] a difference for our nation,"* the forum committed to sharing its thinking with the private sector. In the interim between June and October, members' outreach surpassed their

expectations. Based on feedback from that outreach, the forum decided to refine its messages related to information sharing and assured communications and to continue to work with private-sector leaders outside the forum.

At the meeting, three avenues for rapid action were outlined:

- Refocusing forum efforts to increase both awareness of, and the effectiveness of, the National Response Plan (NRP). This plan, the “playbook of preparedness” is discussed in the Command and Control – Issue Identification section on page four.
- Encouraging the Department of Justice (DOJ) and the Department of Defense (DoD) to exert every effort to make their information exchange models compatible – and encouraging DHS to participate in this effort. This streamlined collaboration between two distinct bureaucracies holds out the prospect for vast improvements in government information technology efficiencies and is discussed on pages four and five.
- Advocating for a civil communications reserve capacity or “communications CRAF.”<sup>2</sup> The design of this mechanism is time sensitive and on a forum fast-track that is introduced in depth on page five.

## Lessons Learned and Recommendations

### Context

Between the forum meetings of June 2005 and October 2005, Hurricane Katrina devastated the Gulf Coast and created a storm surge that breached the levees in New Orleans. Forum members were asked to identify the most pressing lessons learned from the hurricane and to select particular issues that the forum should address. Members prioritized:

1. Clear, improved command and control structures
2. Assured communications capability

During the interim, forum members made good on their commitment to expand the forum’s audience beyond each member’s significant internal constituencies. Forum members led structured interactions with several premier gatherings of business and government leaders, including:

- The National Security Telecommunications Advisory Committee’s Industry Executive Subcommittee (NSTAC IES)
- The CIO Forum and Executive IT Summit<sup>3</sup>
- The Research Board<sup>4</sup>

This private-sector outreach generated sincere support for forum efforts and revealed some private-sector frustration at having few effective means of channeling that support.

---

<sup>2</sup> The Civil Reserve Air Fleet (CRAF) is a public-private collaboration that provides commercial resources to support DoD airlift requirements in emergencies that exceed the capability of the military air fleet.

<sup>3</sup> An invitation-only conference for the leading CIOs and IT executives in the Washington DC area.

<sup>4</sup> A membership organization of CIOs from 100 of the world’s largest businesses.

### **Command and Control - Issue Identification**

Members concluded that, when put the test, the National Response Plan was not executed effectively, despite the intention of its creators that it be “*the operating manual of domestic catastrophic response.*” Members felt that it suffered from an unfortunate combination of its recent introduction (January 2005) and some previously acknowledged shortfalls. There were many key players with authority to respond at the federal, state, and local level, but each appeared to be “*following a different playbook*”. Multiple authorities had vital roles to play, but members indicated that no single authority appeared able to take precedence and, in the absence of clear command and control, the competing plans were often at cross purposes.

Members emphasized the direct correlation between the scale of a disaster and the need for close collaboration between the responding authorities. The confusion of the Katrina response had been predicted by joint exercises in which local, state, DoD, and DHS actors participated. At prior forum briefings, the complications created by the sheer number of decision makers had been discussed frequently. A valuable lesson gained from the joint exercises but lost in the confusion of Katrina was the essential role played by professionals with experience in cross-organizational environments. Acting as brokers and building on a crucial alchemy of personal relationships and organizational insight, they often become de facto hubs for information exchange. Members commented that the absence of such information exchange on the Gulf Coast was one reason for the shortcomings in response efforts.

### **Command and Control - Conclusions and Recommendations**

In response to the problems identified with the NRP, members agreed that command and control must be established ahead of time and that all parties must know their proper roles before a catastrophe occurs. Members committed to re-engaging DHS leadership in a discussion of the forum’s past recommendations concerning the NRP. Members viewed a number of these recommendations as a necessary first step in implementing solutions to many of the problems encountered after Hurricane Katrina. They agreed that providing support to DHS in these crucial early years is essential for domestic security and should be a core mission of the forum.

Forum members also concluded that the forum itself was the kind of collaborative venue that encourages IT executives within and outside of government to identify shared challenges and complementary efforts. At this meeting, several partnership opportunities were identified, including (1) DoD participation in a February 2005 mock cyber attack led by the Office of Science and Technology and (2) alignment of DoD and DOJ information exchange models, including the DOJ’s National Information Exchange Model (NIEM).

The NIEM was introduced at the last forum meeting as an emerging initiative and a framework for standards for information exchange that creates a common language for all levels and branches of law enforcement. DOJ and DHS are using the NIEM as a platform for future applications. NIEM is intended to make possible “national-level interoperable information sharing and data exchange.”<sup>5</sup> While described as “*a beta program for federal data reference with some legs ... and considerable cautions raised by the intelligence community,*” members agreed that it filled a void and merited

---

<sup>5</sup> National Information Exchange Model, “About NIEM: What is NIEM?” <http://niem.gov/aboutniem.php>

further investment. There was support for its intentions and respect for its rapid acceptance, and members agreed to further its progress by directly linking relevant DoD and DOJ efforts in these areas.

### **Assured Communications - Issue Identification**

Another crucial lesson of Katrina – that reliable communications are critical for effective emergency response – was one the forum had previously identified. By coincidence, forum members had completed a white paper on the topic of assured communications a day before the New Orleans levee system was breached. The forum’s appraisal of the state of the nation’s communications capabilities foreshadowed the breakdown of communications that accompanied Katrina. The forum was not alone in discussing the consequences of such communications breakdowns; the 9/11 Public Discourse Project also took up the topic.

“Hurricane Katrina reminds us that the problems of assured communications and information sharing have not been solved. Poor communications delayed emergency response. Poor communications again cost lives. New Orleans and three neighboring parishes were using different equipment and different frequencies – they couldn’t talk to each other. Helicopter crews couldn’t talk to rescuers in boats. National Guard commanders in Mississippi had to use human couriers to carry messages. We should not have to learn these lessons a third time.”<sup>6</sup>

Members also pointed out that Katrina revealed the widely acknowledged gap between innovations in communications technology and applications on the one hand and government appropriations, planning, and strategy on the other. While DoD is widely considered an innovative early adopter of leading-edge technologies, the adoption rates of first responders and other federal, state, and local actors are less consistent. Members observed that leading-edge technologies are readily deployed by businesses at the local level and that this deployment provides a potential platform for an integrated assured communications capability.

Members also expressed concern that in the immediate aftermath of Katrina, well-intentioned appropriations could result in programs and expenditures that do not fully utilize the commercial capabilities that already exist in the marketplace. As one member pointed out, *“The last thing we should do is warehouse emergency communications equipment and PCs all over the country ... industry is producing over two million cell phones a day. We ought to find ways to leverage all the communications capacity that already exists.”*

### **Assured Communications - Conclusions and Recommendations**

Forum members concluded that without an interoperable and assured communications capability, all other response and recovery efforts will be comprised. Forum members urged that communications be considered not just one critical infrastructure (together with power, transportation, health care, etc.) but – at least in the context of emergency response – *the* critical infrastructure that underpins command and control.<sup>7</sup>

---

<sup>6</sup> 9/11 Public Discourse Project, Timothy J. Roemer, prepared statement before the Subcommittee on Telecommunications and the Internet Committee on Energy and Commerce, U.S. House of Representatives, September 29, 2005, <http://www.cnponline.org/spectrum.htm>

<sup>7</sup> The forum’s Assured Communications working paper had previously identified the risks that a Katrina-like situation poses to our nation’s communications infrastructure: severe damage to the wireline and wireless communications infrastructures throughout the

Building on this perspective, forum members recommend the creation of a communications equivalent of the Civil Reserve Air Fleet (CRAF). The CRAF is a public-private collaboration that provides commercial resources to support DoD airlift requirements in emergencies that exceed the capability of military aircraft. U.S. airlines contractually pledge aircraft to the CRAF, ready for activation when needed. In return, the government compensates commercial providers for aircraft use in an emergency and makes peacetime airlift business available to participating commercial airlines. CRAF activation occurs only to the extent necessary to support the DoD's needs.<sup>8</sup>

Forum members propose the creation of a civil communications reserve capability (CCRC) on the CRAF model. The CCRC would make it possible for communications systems owned and operated by commercial providers to be utilized by the government during a national emergency. As with the CRAF, companies would be offered economic incentives to participate in the CCRC, so the government could be assured of access to the necessary equipment, hardware, and software in an emergency. The system could potentially extend beyond voice connectivity and include rapidly constituted and deployable capabilities, such as messaging services, call centers, or websites for collaboration. During a period of CCRC activation, commercial providers would continue to operate the designated equipment, in accordance with predetermined protocols that support DoD, DHS, or other government agencies' missions. Members decided to hold subsequent meetings to refine and advance the CCRC concept.

### **Private-Sector Outreach – Issue Identification**

In a series of meetings that took place between June and October, forum members interacted with private-sector IT leaders. In general, these leaders communicated strong support for the work of the forum, paired with some frustration over how to act on that spirit of support.

In particular, private-sector CIOs said they needed a persuasive way to communicate the urgency of assured communications and information security issues to their CEOs. In the absence of declassified government material, CIOs expressed concern about the viability of carrying specific recommendations forward inside their organizations. In addition, many private-sector CIOs recognize that the private sector needs to do more work on the emergency preparedness and disaster recovery fronts. They suggest that there is an opportunity for public-private collaboration in those areas, particularly in sharing best practices and learning from actual collaborative private and public responses in emergency situations.

In a discussion of the NSTAC and its forthcoming recommendations to President Bush on next-generation networks (NGN), it was clear that while there may be questions as to the when and how of convergence, there could be no doubt that converged networks will be more robust and will offer many advantages. However, one member cautioned that *“new capabilities are usually coupled with new liabilities.”* A first responder, dealing not only with voice capability, but also with street and building maps and key data on chemical holdings, infrastructure capabilities, numbers of occupants,

---

area, flooded switches, loss of power. Perhaps auspiciously, that working paper also identified areas in which attention should be focused and in which solutions to the cascading problems that afflicted New Orleans could be found.

<sup>8</sup> Air Force Link, “Civil Reserve Air Fleet,” <http://www.af.mil/factsheets/factsheet.asp?&ID=173>

types of tenants, and so on, will have the new challenge of managing this information, ensuring its fidelity, and applying it correctly.

### **Private-Sector Outreach - Conclusions and Recommendations**

Ultimately, forum members concluded that the private sector continues to need prodding to focus on homeland security concerns. Short-term awareness is often attached to the most recent emergency, while broader substantive awareness is a long-lead proposition requiring national engagement. The latter is difficult to achieve, and as one member pointed out, requires *“a Y2K-level of national commitment and focus.”* Absent such a commitment, forum members felt that incremental change is possible and suggested that future activities should strike a compromise between raising awareness and providing clear guidance on effective measures that the private sector can implement today.

Forum members agree that the working papers on information sharing and assured communications contain important recommendations; members will continue to develop implementation plans for each. Future forum collaboration with private-sector audiences may focus on identifying those steps in the plans that depend on industry participation. Responding to overwhelming private-sector desire for case studies of best practices, members committed to *“seeking means to partner with industry in the development of disaster scenarios, so that the existing body of government work is complemented by a private-sector perspective.”*

In addition, forum members agreed with NSTAC’s assessment that Katrina revealed deficiencies in restoration and recovery of critical communications infrastructures. Forum members committed to working with the NSTAC, specifically on recommendations that emphasize clear command and control and gains in enhanced information sharing. Members agreed that many of the NSTAC’s near-term recommendations reflected the forum’s prior recommendations and that combining forum thinking with the NSTAC’s efforts would increase the likelihood of successful adoption and implementation.

### **Looking Forward**

Forum members believe that improved preparation is a prudent response to increased risk. Members asserted that it should not take an actual emergency to prompt the nation to learn lessons that might otherwise be learned from past experience and the nation’s vast reservoirs of institutional knowledge. As one member put it, *“If we have two more hurricanes, maybe we’ll be good at responding to hurricanes, but what about cyber attacks, chemical and biological warfare, and other potential catastrophic events? Unfortunately, it seems to take actual catastrophes to force lessons through the system. That cannot be acceptable.”*

The forum refuses to wait for the next catastrophe to become better prepared. *“We mustn’t wait for a pandemic or attack to learn how to be prepared. We must be prepared to respond and, even better, to prevent such events.”* In the coming months, aligning its sense of the national interest with its own particular information technology strengths, the forum will work to assure that in the aftermath of Katrina, it provides prudent guidance on allocation of resources and technologies. Because of their expertise, members will also consider means to build on a widely shared interest by members in accelerating our nation’s cyber attack preparedness. Last, the forum expects to help elevate discussions with national leaders above individual company, agency, or state and local agendas.