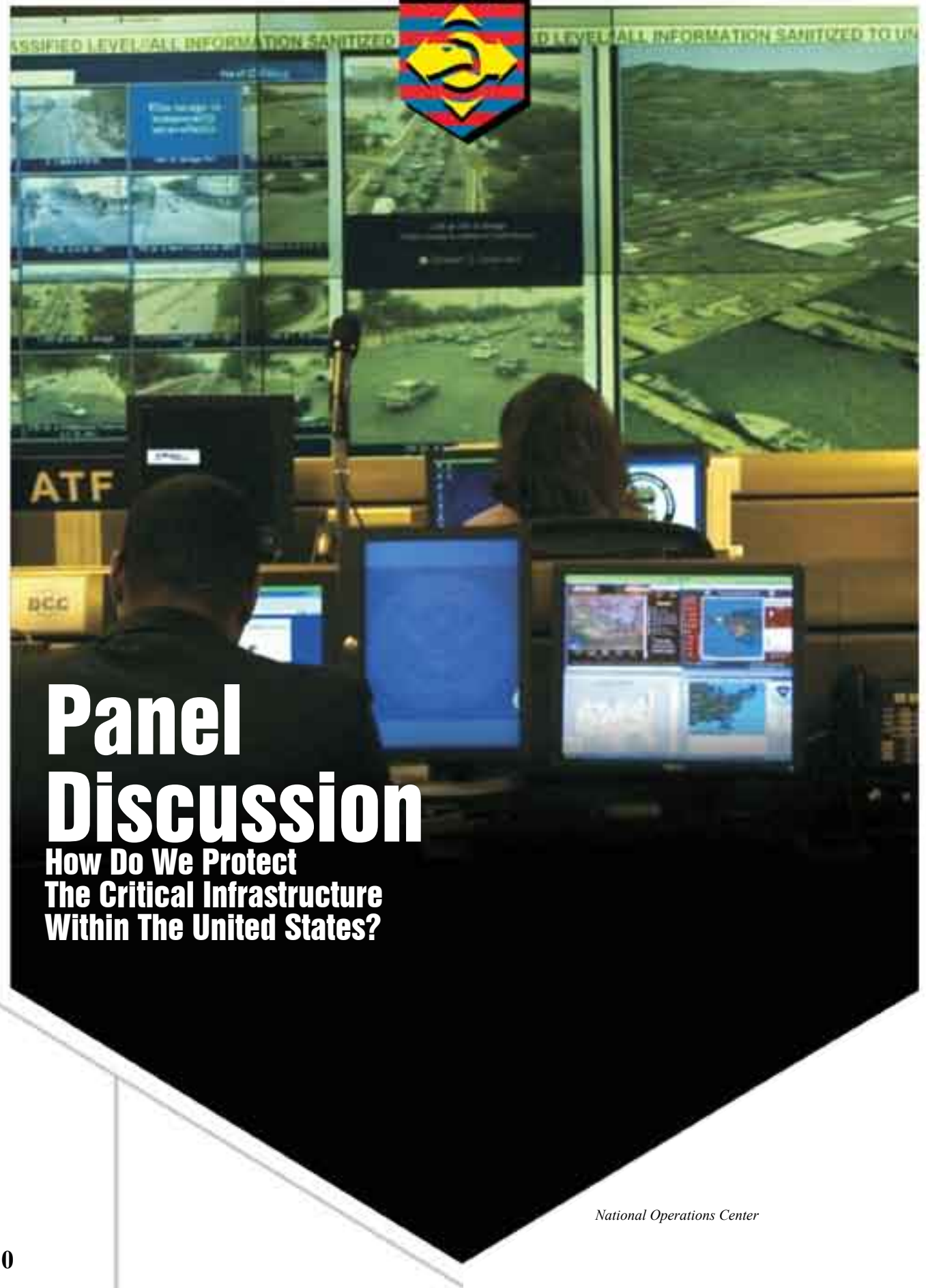

Panel Discussion

How Do We Protect The Critical Infrastructure Within The United States?

National Operations Center

Editor's Note: Critical infrastructure is the backbone of our national economy and is essential to the health, security, safety and economic well-being of our nation. Don L. Rondeau, President and CEO of Total Security Services International, Inc. (TSSI), IACSP Board member and President of the IACSP's Washington DC chapter, recently gathered a team of national homeland security experts and professionals to discuss the current challenges faced in protecting critical infrastructure within the United States. In this dynamic and thought-provoking roundtable discussion, these leaders discuss how to identify and assess emerging threats and how our nation can enhance its ability to protect Critical Infrastructure and Key Resources (CIKR) whose destruction, incapacity, or degradation would have a debilitating impact on our nation's safety and security.

Panel Discussion

Mr. Rondeau:
First and foremost, thank you all for your outstanding contributions to securing our homeland and its valuable resources. I am extremely privileged to have such a stellar team of thought leaders and experts to offer as a resource to both our clients at TSSI and its parent company, Macfadden. Several of our panelists are currently serving as members of TSSI's Critical Infrastructure Protection Strategic Advisory Group and we also have our team of trainers in our midst who specialize in the transportation sector and are here to provide valuable threat and vulnerability assessment expertise.

As each of you is aware, there is a tremendous level of interdependency among the various sectors of critical infrastructure. The cascading affect of a natural disaster or terrorist attack is inevitable due the nature of these dependencies. How does this interdependency affect our ability to plan and prepare for these types of events?

Major General (Ret) Arnold:
The interdependency piece will always be there and there is no way to really get around that. Today, all of the parts and pieces are brought together through our information and communications systems. Into the future, it will be critical to recognize this interdependence. Through communications and information we can allow that interdependency to become more transparent.

I would also like to point out that when we speak about critical assets, the most critical asset that I think of is our people. We don't normally think about people as an infrastructure resource, but people are the most important resource that we have. It takes people to do everything else.

I would also like to point out that when we speak about critical assets, the most critical asset that I think of is our people. We don't normally think about people as an infrastructure resource, but people are the most important resource that we have. It takes people to do everything else.

Capt. Brown:
Our country is absolutely transportation and information dependent and there is virtually nothing that can be done in isolation the way our economy and our industrial base is set-up. We are dependent on just in time stocking, and as such, we are never really more than 3 to 4 days away from food riots. For example, if our transportation systems were to break down, or trucks stopped for inspections and not permitted to move, the implications would be devastating. Furthermore, our critical infrastructure tends to have endpoints within very populous areas. As a result, what affects one area, affects others. It's really not just what may happen in a given industry, or to a given structure, but what happens near it, in it or around it.

Mr. McHale:
I think we've come a long way over the course of the past 7 years. In looking at the interdependencies we've uncovered many dependencies we had never known to exist. We also have a much greater understanding of the nature of the terrorist threat.

Mr. Beatty:
The key to protecting critical infrastructure and ensuring continuous delivery of services is identifying single points of failure. Often implementing a redundant capability is a more economical and efficient response. For example,

Don L. Rondeau
Moderator
As President and CEO of TSSI (www.tssi-inc.com), Don L. Rondeau oversees the development of new business opportunities in the homeland security arena, focusing on transportation safety, asset protection, contingency planning and conflict mitigation. Mr. Rondeau also serves as Senior Vice President of Critical Infrastructure at Macfadden, parent company of TSSI. Mr. Rondeau's expertise spans a broad and distinguished career in the area of critical infrastructure protection.

Panelists:
Joe M. Allbaugh
Joe M. Allbaugh served as Director of the Federal Emergency Management Agency (FEMA) from 2001 through 2003. As head of FEMA, Allbaugh coordinated the Nation's $8.8 billion response and recovery efforts in the traumatic days following 9/11 and received much public acclaim for his leadership of FEMA. He is also a founding member of the President's Homeland Security Advisory Council. Mr. Allbaugh currently serves as President of Allbaugh International Group, LLC.

Major General (Ret) Wallace Arnold
Major General (Ret) Arnold possesses a wealth of leadership, command and operational experience. Culminating his Army career as Assistant Deputy Chief of Staff for Personnel, he has continued a successful private sector career since his retirement in 1995. Major General (Ret) Arnold served as director of the Hampton University Data Conversion and Management Laboratory, and as Interim President, Cheyney University of Pennsylvania. He received an Honorary Doctorate of Law from Campbell University.

Stephen J. McHale
Stephen J. McHale is co-chair of Patton Boggs, LLP, Homeland Security, Defense and Technol-

ogy Transfer Practice Group. Mr. McHale brings 24 years of government service and experience consulting clients on national and homeland security matters. As the first deputy administrator of the U.S. Transportation Security Administration (TSA), he played a key role in federalizing aviation security after the September 11, 2001 terrorist attacks and has played a key role in working with government leaders to develop critical infrastructure protection plans within the U.S. Department of Homeland Security.

Jeff Beatty

As founder and former president of TSSI's predecessor organization, Jeff Beatty continues to serve as a Special Senior Advisor to President and CEO, Don L. Rondeau at TSSI. A former Delta Force Assault Troop Commander and Operations Officer, Mr. Beatty later served as an FBI Special Agent and advisor to the national Hostage Rescue Team (HRT) and as a CIA Counter-terrorism Center Case Officer, where he successfully managed anti-terrorism operations in Europe and the Middle East. A renowned anti-terrorism expert, the U.S. Senate sought his testimony regarding transportation security issues, including aviation, following 9/11. He authored the Anti-terrorism Action Plans for the American Trucking Association and the American Bus Association. Mr. Beatty predicted the Atlanta Olympic Bomb and warned all U.S. Airlines in 2000 to harden cockpit doors and change procedures relating to apparent hijackings.

Capt. Raymond Brown (Ret)

Capt. Raymond Brown offers specialized maritime and land security experience and possesses unmatched threat vulnerability and assessment and security awareness training experience. A former Chief of Analysis in the U.S. Coast Guard's Intelligence Center and White House military aide, Capt. Brown has developed several highly successful anti-terrorism training programs within the transportation sector, including courses for the American Bus Association, the Massachusetts Turnpike Authority and Logan Airport.

Col. John S. Rogers (Ret)

Col. John S. Rogers has extensive security and force protection experience and has conducted numerous international threat and vulnerability assessments in volatile areas around the world during his service as a U.S. Marine Corps officer, including Korea, Bosnia and Kosovo. Additionally, Col. Rogers led training course development for the Federal Motor Carrier Safety Administration's (FMCSA) Safety Investigators and has conducted threat assessments on behalf of the National Park Service and the USS Constitution. An expert in security-related issues Col. Rogers is adept at identifying vulnerable infrastructure and developing appropriate security plans.

Edward J. Boekenkamp

A former U.S. Marine Corps officer, Edward J. Boekenkamp has spent more than 30 years leading numerous security initiatives. Having trained more than 30,000 individuals since 9/11, he has a breadth of experience in the international arena and maritime operations. He has conducted critical vulnerability and threat analysis assessments for international firms in addition to state and federal infrastructure.

while working as a consultant with an emergency services command center in a challenging environment with difficult terrain, we found there was no back-up or failover system in place. The cost of hardening this single point of failure was excessive, but the cost of creating redundancy or an alternative capability was significantly less than protecting the single site of infrastructure itself. Sometimes even after spending millions of dollars on high-end security solutions, you may have done all you can to reasonably protect site "A" when what you really need is an alternative site "B".

Mr. Allbaugh:
We cannot ignore our infrastructure. It is the key to our economy, key to our freedom and key to our mobility and our security. We are at risk, and the most important thing that we as Americans can do is to not become complacent. We have to reach out and make sure that our employees are involved with this effort from the private sector to interact with appropriate government agencies to make sure there is a proactive approach to understanding our infrastructure and devising ways to protect our weakest components.

Mr. Rondeau:
Single point vulnerabilities are a fundamental concern when evaluating infrastructure vulnerabilities. How can we avoid having an Achilles' heel or single point of failure within our infrastructure?

Capt. Brown:
We must avoid a single point of failure by building in alternate sources or back-up redundancies. Unfortunately, all too often this point of failure does exist. Sometimes it's a technology or mechanical aspect – sometimes a location.

Major General (Ret) Arnold:
I'm not sure that we have a single point of weakness. If there is one, it's probably between the connectivity of our communications systems – being able to communicate on key aspects of infrastructure vulnerability and risk to certain things. The more we improve our communication the better off we can be. We can reduce risks and be able to react better to our planning processes if we obtain information in a timely manner.

Mr. McHale:
There is ultimately no way we can have an open society and open economy and not have areas of vulnerability and risk. We don't have resources for 100% protection to prevent 100% of threats, and we never will. Nor do we want to live in the type of society that supports this. What we really need to do is build a resilient system. We actually have a pretty resilient infrastructure in place in that there are very few real choke points that can't be worked around fairly quickly. However there are still choke points.

Mr. Allbaugh:
Once you identify 100 points of weakness or 20 points of weakness, you have to prioritize where these weaknesses are and immediately set about executing a plan to make sure there is not a single point of weakness anywhere. We have to identify them and execute a plan immediately to make sure that the weakness only becomes a manageable vulnerability.

Mr. Rondeau:
What can we do to ease the cascading effect of an attack or disaster that affects this infrastructure?

Mr. McHale:
The biggest danger during the immediate aftermath is the danger of overreaction. For example, in the immediate aftermath of 9/11, there was a lack of information and understanding about what had happened. The entire aviation system was shut down along with a number of other measures taken. Tunnels were shut down; the movement of hazardous materials on railways was slowed. All sorts of unrelated and uncoordinated actions severely affected both our economy and our ability to respond.

In the immediate aftermath, we must have a plan to prevent hurting ourselves more that we have been hurt by the attack itself. In the longer term, we must carefully reassess what vulnerabilities have been uncovered and make sure they are taken care of and prepare for whatever may be coming at us next.

Mr. Allbaugh:
Now that we're 5 years, 9 months beyond the creation of the Department of Homeland Secu-

rity, there's been a mindset and reluctance to share information. I think it is most important for federal state and local governments to intersect with private infrastructure to identify those weak points and share that information. If we don't know where the weak points are, it is really hard to devise a plan against nimble and agile terrorists. We have to start with that basic database. There have been several attempts over the past 5 years, but not all of the information has been shared properly. What people in Washington or other federal sites around the country may think is critical may not be the same as what the local folks think. So there really has to be an agreement on the database and then we must devise a plan to protect those weaknesses.

Capt. Brown:
The most important thing is to recognize that it can happen and be willing to take time to not only plan for these types of events, but also to train people and actually exercise the plan. In many industries, businesses, port authorities, transportation authorities, etc., contingency plans may or may not exist. If they do, they may not have been updated. In the wake of 9/11 and Katrina, many were shaken out of their lethargy, but as time goes on, people become more concerned about the bottom line. A generation ago, the mantra that safety is everyone's job became important. The thing to do now is to be sure that a new mantra evolves and that it becomes part of everyone's mindset that security is everyone's job.

Col. Rogers:
Our work within the transportation sector has helped understand the potential impact of infrastructure damage. It affects the entire economy. The key is helping understand potential impact. We must help people realize time is money and help them to feel part of the solution.

Mr. Rondeau:
How can we more effectively identify threats and risks and assess our vulnerabilities?

Capt. Brown:
We must always identify threats, most always originate from the outside, and vulnerabilities, or weaknesses from within. When your threats meet your vulnerabilities that is when you have a real problem. We must then work to identify responses and prioritize vulnerabilities. Finally, given that we can't solve everything at once, we must prioritize limited resources.

Most importantly, once we've done all of these things, we need to teach people how to think about safety and security. It's a continuous loop, you must keep revisiting it. It needs to become a way of life, just like safety has become a way of life for most industries in the U.S.

Major General (Ret) Arnold:
We have to build in as much redundancy as we can to allow continued operations. It is essential that we do not put all of our eggs into one basket. We must look at alternative routes and means. Modeling and simulation is key. We need to use more simulated environments to train in. Future systems should target key critical infrastructure assets to replicate and then train against these.

The most common challenge today is always resources, whether lack of time, money or people. There are many ways to help protect against threats using technology or personnel. Sometimes simply updating plans with security policies and procedures that better protect critical assets is a much more cost-effective alternative.

Col. Rogers:
In the 21st century we know one of our greatest threats is from terror. It's also critical to take an all-hazards approach and not just focus on terrorism. For example, during natural disasters, critical infrastructure is always vulnerable. The key is to have a general idea of potential threats and our own vulnerabilities and be cognizant of whether those threats will actually exploit our vulnerabilities. If the two marry, that's where you should put your resources. The best thing to do is to start by conducting a threat and vulnerability assessment. Realize that you have vulnerabilities and look at the known threats. Then see what you can do to make it "not happen" and prioritize what can reasonably be done with limited resources.

Mr. Rondeau:
How can we better prioritize threats with limited resources?

Mr. Beatty:
The best thing we can do is have a thorough understanding of the threat and work with those who have demonstrated a superior knowledge of threat capabilities and our own capabilities. Then we can better prioritize your limited dollars to address the vulnerabilities that are most likely "real" risks. It is important to understand that you don't have to make your security perfect… By simply moving that vulnerability to the "too hard to do" category, where the attacker cannot be certain of success, we can significantly reduce our vulnerability by making an attack not worth the operational energy required where there is no guarantee that the attack will succeed. As a part of this strategy, we can channelize the enemy into performing certain necessary precursor "Operational Acts" and put training and technologies in place to detect those "Operational Acts." Thus giving security forces increased opportunities to detect and defeat attacks before they are pressed home...

Col. Rogers:
The most common challenge today is always resources, whether lack of time, money or people. There are many ways to help protect against threats using technology or personnel. Sometimes simply updating plans with security policies and procedures that better protect critical assets is a much more cost-effective alternative.

Major General (Ret) Arnold:
I don't necessarily agree that resources are limited. We have access to fairly vast resources. It's more a matter of how we use those resources. For example, we have a number of intelligence gathering organizations but a number of them are still stove piped and lack an essential cross feed of information that would allow threats to be recognized and allow analysts to work with more information. We must continue to create transparency and break down these information silos. It's not so much that we don't have the resources; it's really how we bring them together for a common good. We must share information and establish standards.

Mr. McHale:
It's always a question of getting timely, operational intelligence to law enforcement and others who need to act on it. We need to get meaning-

ful, timely information out to industry security officers and officials so they are able to act on the information and build it into their planning allowing them to identify real risks and allocate resources toward those risks. If we just tell someone to protect themselves against all risks, they're not going to protect themselves very well against any risk. If we tell them to protect themselves against particularized risks they are much more likely to take effective measures to protect themselves.

Mr. Rondeau:
How are technologies such as modeling and simulation, among others, improving our ability to identify threats?

Capt. Brown:
One thing that concerns me is that many organizations are selling technology solutions as though they are a silver bullet. I personally don't think there is one. Yes, there are great tools out there. It's the American way to look for a technological solution. But when it comes down to it, the human mind is our greatest weapon. With extensive experience in critical infrastructure and security, these experts can take a hard look and see what needs to be done. These tools need to be evaluated for their intrinsic value, but it still takes trained people who know how to think about threat and vulnerability.

Mr. Allbaugh:
I am so proud of the private sector and their ingenuity. What is frustrating to me is that our government is often extremely reluctant or just flat out fails to embrace new technologies that are available. There has to be a mechanism for these technologies to come into our federal government in order to be adopted, employed or deployed. It takes a huge amount of networking to get in front of decision maker – it takes time. A lot of folks think that is good because it takes time to have the best technologies rise to the top. I'm all in favor of the best technologies becoming the cream of the milk, but we have to balance that with being expeditious and making sure the latest and greatest technologies are used to protect our infrastructure, protect our services and protect our citizens and our borders.

Mr. Rondeau:
Nearly 85 percent of our nation's critical infrastructure is presently owned by the private sector. How can we encourage and develop partnerships between industry and government? How are these partnerships central to the success of our protection of critical assets?

Col. Rogers:
Our government has done a good job taking steps to improve this. An educational outreach program is really needed to help private industry understand the interdependencies of our infrastructure and understand that we're all in this together and working toward a common goal. Our work with the trucking industry within the transportation sector has really heightened the awareness of the potential impact infrastructure damage can have on the economy as a whole. We need to help industry realize our infrastructure is extremely interrelated and help them feel like they are part of the solution.

Mr. Allbaugh:
The consolidation of committees of authority in Congress is a huge step in the right direction. It is imperative that Congress takes steps to ensure that FEMA is able to perform and act expediently without interruption. That means FEMA should have the authority to respond to man-made or natural disasters with ability to perform emergency tasks and services at the time of disaster without having to go through too many layers of bureaucracy. FEMA has taken the right steps to reach out to the private sector and organize critical partnerships. There are programs being coordinated by FEMA today, that are very successful and that saves lives. However, with more budget and personnel, it can become even more successful. The private sector holds the keys to the information on the ground. Effective actions by governmental agencies rely, to a large extent, on this information. Greater cooperation between both will lead to efficiency, and most important, to saving lives.

Mr. Boekenkamp:
Our biggest potential for weakness occurs when we fail to involve American citizenship. Our work with the "First Observer" trucking security program in conjunction with the Transportation Security Administration is an excellent example of the type of grassroots efforts that can be very effective. No we do not have all of the assets and resources that we require and we never will. Industry partnerships will be key, but we also need to extend our efforts down to the level of our citizenry. Observe and report. At the end of the day, that's what it comes down to. We can have all of the security in the world and all of the latest technological advances, but if the citizen's of our great country don't feel part of the dynamic process, we're going to lose something there.

Major General (Ret) Arnold:
There must be some policy breakthroughs. To achieve a level of real collaboration we must establish policies, procedures and standards and then we can begin to create transparency between the public and private sector.

Capt. Brown:
The partnerships are being developed, but not to the extent necessary. The federal government has fostered partnerships through the use of grants to benefit municipalities, urban areas and various transportation authorities. The private sector has been hauled in at the margins, but this is still embryonic in the U.S. Through additional grants, tax incentives and training projects we can further develop these partnerships.

Mr. McHale:
These partnerships are essential. We must continue to remind people and advise the private sector about the types of risks they are likely to face and let them know the cost of not being prepared. Most importantly, we must continue to share information. Unless, we get the information out to those who need it, we're not getting the value from the information.

Mr. Beatty:
We have to do more low-cost, high-value things. We also cannot paint civilian owners of critical infrastructure into a liability corner. We must train people to increase security awareness. Increasing the number of eyes and ears is not overly burdensome. Outreach is essential to educate and sensitize people to understand our new world. By giving them a new awareness, we teach them to observe and report things and alter their default tendency to rationalize irregularities and believe a reasonable explanation must exist. The new default position must be to report ANY irregularity.

Mr. Rondeau:
What steps should we be taking to continue enhancing our nation's preparedness?

Mr. Boekenkamp:
At TSSI we've laid down a pretty good template. We have an enviable history of providing training vulnerability analysis, identifying vulnerabilities, and risk management matrix and have tailored solutions from here. We're not totally there yet nationwide, but it's going to be an ongoing endeavor as threats continue to evolve.

I keep going back to the deterrent value. If we can continue to exert intelligent pressure, the results will be incredible. By engaging people we improve our preparedness.

Col. Rogers:
Our nation is really good at being reactive, but we really need to become more proactive. We are not completely there yet, but national efforts in the post - 9/11 period have contributed to an enhanced ability to proactively anticipate, deter and defeat threats before those threats manifest into actions that adversely impact critical infrastructure and key assets.

Major General (Ret) Arnold:
We need to continue to improve our intelligence networks and have resources be more transparent and improve sharing of information. We must continue to build redundancy for critical systems and improve international networking to facilitate a real exchange of information.

Mr. Rondeau:
The reality is that we continue to be surprised by disasters and terrorist attacks more than we should. This proven group of leaders is adept at responding to terrorist threats, matters of national security, high level strategic training missions and has demonstrated a unique ability to actively engage the private sector. To continue on a positive path toward improving the security of our most valuable assets, we must be more than program managers and more than security experts. We need to continue to integrate best-in-class science and put critical information in the hands of those in charge of responding to an event. As a nation, we are continually improving our ability to analyze intelligence and improve processes that save lives, alleviate suffering and protect our nation's assets and people.