INCIDENTAL PAPER

Seminar on Intelligence, Command, and Control

The National Infrastructure Protection Center

James B. Plehal

Guest Presentations, Spring 2002

Robert B. Brannon, Gregory C. Radabaugh, Robert A. Rosenberg, Gary L. Salisbury, Roberta E. Lenczowski, James B. Plehal, Dean W. Cash, Patrick F. Kennedy, Warren B. Rudman, Joseph K. Kellogg, Jr.

January 2004

Program on Information Resources Policy

Center for Information Policy Research

Harvard University

The Program on Information Resources Policy is jointly sponsored by Harvard University and the Center for Information Policy Research.

Chairman
Anthony G. Oettinger

Managing Director
John C. B. LeGates

E-mail: pirp@deas.harvard.edu URL: http://www.pirp.harvard.edu
ISBN 1-879716-81-X **I-02-1**

The National Infrastructure Protection Center

James B. Plehal

March 21, 2002

At the time of this presentation, Rear Admiral James B. Plehal, U.S. Naval Reserve, was deputy director of the National Infrastructure Protection Center (NIPC), and commander of the Naval Reserve Security Group (NRSG) Command.[1] In his civilian career, he is an assistant vice president and financial consultant with Merrill Lynch. After early assignments in weapons, communications, operations, sonar, and supply, and teaching naval history, communications, and tactics at the U.S. Naval Academy, he began his cryptologic career as a special duty officer (cryptology) at Naval Security Group Activity (NSGA), Homestead. His assignments included serving as direct support division officer, where he provided support to deployed units in the theater and participated in the first surface deployment into Soviet home waters. He joined the NRSG after leaving active duty in 1979. His reserve assignments included command of units in Wisconsin and Minnesota. He also served the readiness commander, Naval Reserve Readiness Command Region Sixteen, as special assistant for cryptology and in 1995 was appointed as the first reserve cryptologic area coordinator central, with responsibility for seven NRSG units. His reserve training assignments have included tours with the Naval Security Group Command; National Security Agency (NSA); Naval Surface Reserve Force; the commander in chief, U.S. Navy, Europe; Office of Naval Intelligence; Defense Intelligence Agency; commander of naval forces, Korea; and NSGA Hanza, Okinawa. He graduated from the University of Utah with a B.A. (honors) in political science and a certificate in international relations. He is also a graduate of the Senior Naval Reserve Officer Orientation Course, National Senior Cryptologic Course for Reserve Officers, and Senior Intelligence Leadership Symposium, and attended the Naval War College and Defense Intelligence College.

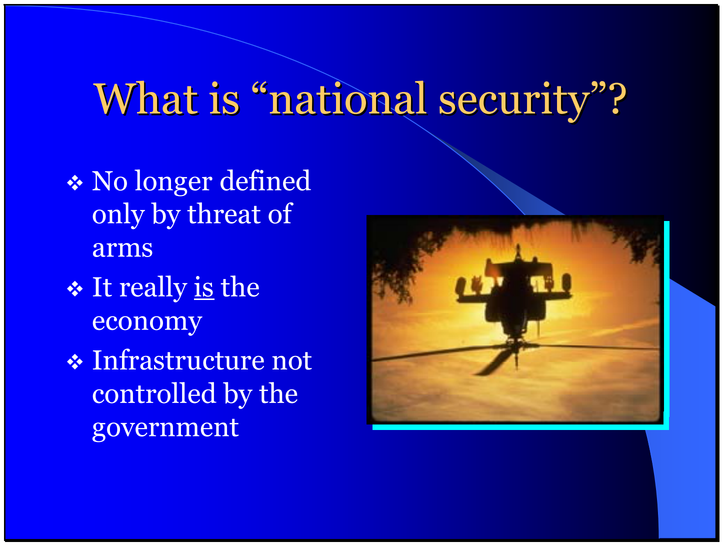
Clemons: On behalf of the seminar and of Tony Oettinger, who can't be here today because of illness in his family, I would like to welcome today's speaker, Admiral James Plehal. You have all read Admiral Plehal's biography, so I won't go into detail on his background. You have also read

[1] Admiral Plehal served as acting director of the NIPC from December 2002 until March 2003, when the Center became part of the new Department of Homeland Security.

the executive order that stood the NIPC up, so you should know a little about that as well.[2] With that, Sir, it's all yours.

Plehal: Thank you for inviting me here today. As you know, my background is as a Naval Reserve cryptologist, and I came out of retirement a year ago to serve as deputy director at the Center. I don't want to give a presentation; I think we're here to talk and discuss. Of the slides I have, a number are what I would call a NIPC primer. They cover what the NIPC is, where it comes from, what it is supposed to do, and how it is structured. Rather than try to get through all this, I'd just as soon have you interrupt me any time with any questions you might have so that we can go more into them. They may be more valuable than what I have here anyway. What I wanted to do was just give you a quick context with the first two or three slides and get through those, and then we can start to address your concerns.

Basically, we in the military think about national security as keeping the hordes off the beaches and not letting foreign armies into this nation (**Figure 1**). That certainly developed after the Revolutionary War and the War of 1812, and carried over into the twentieth century when we had the two World Wars. Of course, the First World War wasn't at all on our beaches, but in the second there was a question as to whether that would happen. After World War II came the NORAD [North American Aerospace Defense Command] scheme of keeping our airspace free of incoming missiles. It wasn't just soldiers coming in; it was missiles that could come in with payloads. That's how the Department of Defense [DOD] generally has looked at things, as we have looked at them as a nation.



What is "national security"?

- ❖ No longer defined only by threat of arms
- ❖ It really is the economy
- ❖ Infrastructure not controlled by the government

Figure 1

[2] *Critical Infrastructure Protection in the Information Age*, Executive Order 13231 (Washington, D.C.: The White House, 16 Oct. 2001). The text is available on-line at http://www.fedcirc.gov/library/legislation/executiveOrder13231.pdf (Accessed on 9 Dec. 2003.)

However, now in the new age—the information age—it's no longer just the threat of arms and soldiers and missiles. It really *is* the economy. The last bullet there I think is very important. This is recognized by the DOD, which is why they have me and others at the NIPC. It is that the infrastructure upon which the DOD and the armed forces rely is no longer controlled by either the government or the DOD. This is true both domestically and internationally. I want to make sure we include the international component today, because when we send our fleet anywhere, its support infrastructure often relies on foreign power, foreign water, foreign logistics, foreign transportation, and the like. Even in this country, the estimate is that 90 percent of the infrastructure is not owned by the government, but depends on private industry to deliver the goods.

The NIPC grew out of a study by a presidential commission formed by the Clinton administration. The commission reported out, and President Clinton signed Presidential Decision Directive [PDD] 63 in May 1998.[3] The NIPC was actually formed a couple of months prior to the publication of the PDD, but the PDD was the driver for it. PDD 63 was the genesis of the government's thinking about critical infrastructures. This is where we defined critical infrastructures—"those physical and cyber-based systems essential to the minimum operations of the economy and the government." So we get "the economy," and "economy" is another term for "our way of life." The way of life is very important.

Clemons: Sir, how are DOD installations abroad viewed in this construct? Are we talking only about infrastructures in the continental United States, or are the infrastructures at Ramstein Air Force Base in Germany considered critical and involved in your domain?

Plehal: They are not within the purview of the NIPC per se. They are the national responsibility of Germany, the host nation. The DOD needs to identify those systems and work with the host countries to ensure that they understand the interdependencies and the critical infrastructure that is providing support to our installations.

The Italians are very interested in this. The Italians, as you probably know, have the Winter Olympics in four years, and have asked the United States—the State Department, the NIPC, and others—to go over and meet with them this spring. Their hook for getting us over there wasn't just the Olympics; it was supporting the Sixth Fleet out of Naples and the infrastructure in Italy that supports our armed services.

It's a good question, because infrastructure does all fall under one umbrella. It is all interconnected. It is all the same. The DOD's interest in the German, or Italian, or Japanese infrastructure that supports U.S. forces is ultimately important to our economy, our way of life, and our national security. The DOD will take it upon itself to look at those issues and bring all of them in, because it's a DOD function to know what their vulnerabilities are. They all feed in, and they're all interconnected.

The PDD identified the eight critical infrastructure sectors that were considered integral to our security (**Figure 2**). It's interesting that when you look at these infrastructures you can

[3] *Protecting America's Critical Infrastructures*, Presidential Decision Directive 63 (Washington, D.C.: The White House, 22 May 1998).

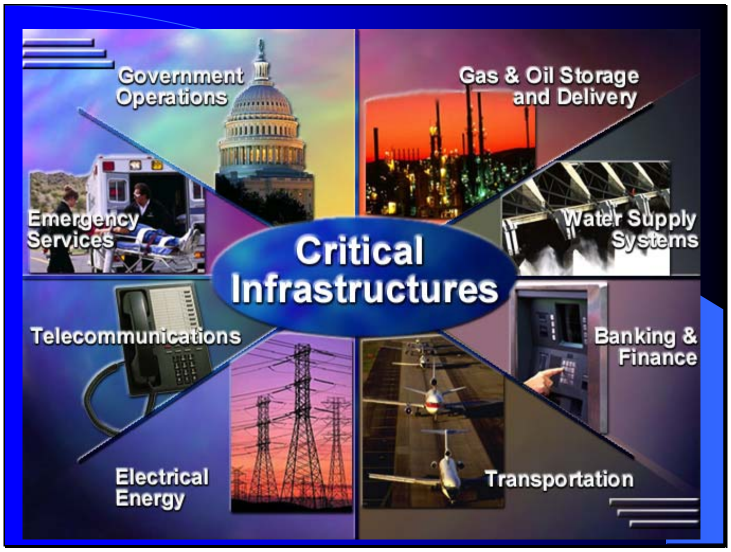


Figure 2

obviously tell why they're critical, but since 9/11 other infrastructures have come in and said, "How come we weren't included in the first place? Aren't we critical?" One that has most recently been knocking on the door is the food industry. So we say, "Of course you're critical, and yes, you should have some of the same capabilities for sharing information." They've probably surpassed other sectors in aggressively taking an interest in providing the government with information on particular threats to their infrastructure from a nationally centered perspective. But I think these other sectors are pretty obvious from the start. "Government operations" may be less obvious, but it includes command and control and provision of services that people count on. If you don't have government operations, then you're running without leadership or services, and things become chaotic very quickly. The same is true of the emergency services sector.

If we look at transportation in particular, there are subsectors. The Federal Aviation Administration is as different from railroads as water is from oil and gas. The subsectors are saying, "We don't want just the Department of Transportation to filter information that applies to all the transportation sectors. We want our own information sharing arrangement with you." So they're starting to break out more as individual subcomponents, and we'll see a little later what they're trying to accomplish.

I've alluded to some of this already, but critical infrastructures have several points that we need to evaluate when we talk about them. They are *interconnected*, and in fact cyber is one of the pieces that interconnects them. You notice that the Internet is not considered an infrastructure. Telecommunications is, but cyber is really an enabler, not an infrastructure by itself. It's one of the ways in which the different infrastructures are interconnected.

They're also *interdependent*. If you lose water, then many times you may also lose your power plant, which then results in a chain of events. That gets to the *cascading impact*. You really have infrastructures that cannot stand alone, because something else needs to serve them. You need to stop looking at them only as pieces, and also look at how they link together. That's why you have those eight critical infrastructures.

Clemons: Does the NIPC have a strategic plan for cascading impacts? Do you run a scenario to determine at what point you would intervene? Is that a normal function of what you're doing, or do you hope to do it at some point?

Plehal: It should be. It is not at this point, and this is because the Center has been focused on cyber, not on the rest of the infrastructures. That's because of resourcing. The Center is a fairly small place, and it has primarily focused on the cyber pieces, and so it has not delved as deeply into the interdependencies and the cascading, although we're aware that we need to focus on them.

There are some initiatives in place that will beef this piece up. In fact, the National Laboratories at Sandia and Los Alamos have a computer capacity in which they do simulation and modeling, and they've put together what's called the NISAC—National Information Simulation and Analysis Center. They're trying to use the excess computer capacity that they used for nuclear power to model infrastructures, which can be very technical and almost never ending. For instance, they've modeled what would happen if there were a flood in Fort Worth, Texas, and tried to see what infrastructures would be affected. A real-world example of that was the Houston flood in June 2001, which I think caused interruption in ATM [automated teller machine] service in twenty-two states, because there was some critical component there. It just goes on and on. Things that you don't think are related all of a sudden are related in some capacity.

The first step in this, of course, is that you have to have the information on where everything is, and that is a big task. Once you have all that information, you can start building your model of what happens if X, Y, and Z take place. I think we'll start getting there, but at this point there is no capacity for that nationally, other than what the labs are doing. The DOD has a component that looks at infrastructures from a protection standpoint. We talked about Italy and Germany and others, but they have done that somewhat in the United States as well because they're concerned about their reliance on U.S. infrastructure. For the most part, this is in its infancy.

I took this slide out of any briefings I gave earlier, because people might think we were paranoid about things (**Figure 3**). This really describes what interconnection and interdependency are and what a multiphase attack on the United States by a foreign power, a terrorist group, or even a criminal group might be like. Then 9/11 came and made it seem a little more relevant. If something happens in one place, something in another, and something in another, maybe it is a cascade, or maybe it is an attack orchestrated by a fairly strong adversary at whatever level, which really would cause disruption in several areas and make us worry about our safety, not just in New York or Washington, D.C., but around the country. The question is, "Are these associated attacks? Are they connected with one another, or are they just random and serendipitous?"

Clemons: How would the Office of Homeland Security mirror or super-set this? I see a lot of those responses as being in Homeland Security.

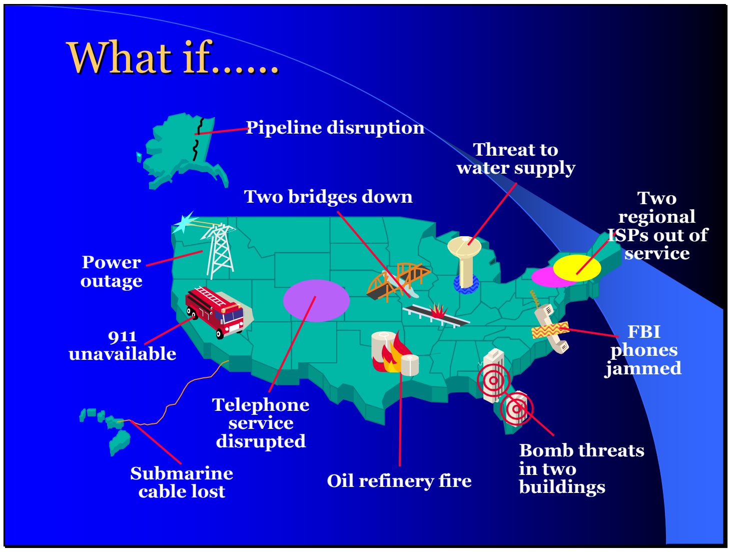


Figure 3

Plehal: Yes, they are. We're going to talk a little more about homeland security, but this might be a good time to introduce the problem, since you're thinking about it. If you look at Executive Order 13228, the Office of Homeland Security does not deal with earthquakes and fires and natural disasters.[4] It does not deal with foreign power involvement in this country. It deals with counterterrorism. The whole executive order is written on counterterrorism. It's fairly narrow. You could say, "We don't know if it's terrorism, a foreign power, or a criminal group," and that's true.

The answer is that the Office of Homeland Security is going to be very interested in this, no matter what the source is, but Homeland Security is really focused on terrorist threats to the infrastructure, not on foreign power threats. That could be one of the weaknesses, or one of the strengths. It's an area that your group may want to continue talking about after today, because how we integrate that component with the broader area is going to be very important. It shows you that there has to be communication. The DOD would be interested if the source of an attack were a foreign power. If these things were initiated by a foreign power, that's a function of the DOD—of Northern Command. If it's a terrorist group, how do you pass on to the next stage and find out what it is? These are some interesting issues.

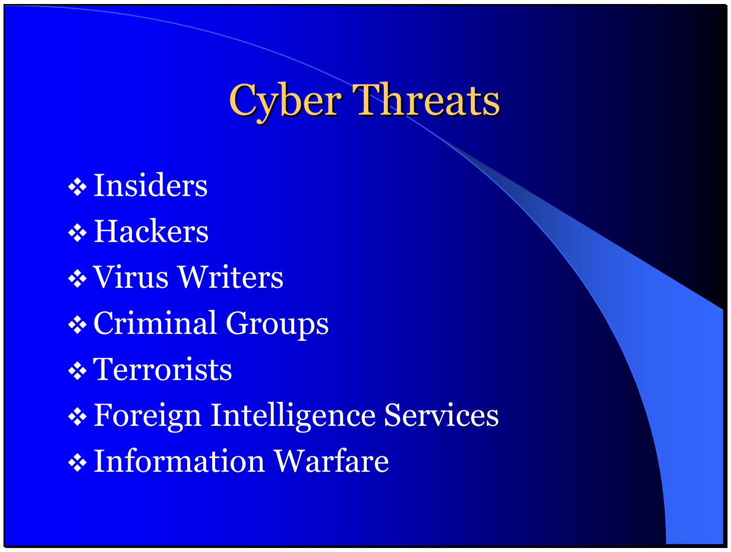
Clemons: I guess the question I was trying to raise for the class is that if there are multiple incidents, there's going to be a clash of organizations that will study that initially, and then the handoff or shakeoff exchange to the responsible agency or center. Potentially, that's going to be really difficult.

Plehal: It would be based on how we have run our government in the past. The trick early on is to make sure it's not a clash of "This is my rice bowl, and that's yours," but that it's "Are we as a government organized to handle this kind of thing in a seamless way?" We have to be sure that

[4] See *Establishing the Office of Homeland Security and the Homeland Security Council*, Executive Order 13228 (Washington, D.C.: The White House, 8 Oct. 2001).

whoever has the information will exchange it so that the parties that have to act, either to mitigate the attack or destroy whoever is doing it or stop it and reconstitute our assets, are all working together. That is the kernel of everything right there, and that's what we've got to deal with.

I want to switch to cyber (**Figure 4**). As I mentioned, the NIPC really grew as a cyber protection center in terms of how it's employed, even if that's not exactly its narrow mission. I wanted to give you the list of what the center considers to be our cyber threats. If this were a DOD slide, a couple of things would be missing from it. One is insiders. General [James D.] Bryan, at JTF-CNO [Joint Task Force-Computer Network Operations], does not have insiders on his cyber threat slide. That's apparently because the DOD is not as worried about insiders, although they must always be considered. The DOD doesn't identify the threat quite the same way. It's looking externally. But when we as a center look at our national picture, insiders are a huge piece. In fact, 78 percent of the money lost from cyber types of incidents is due to actions by insiders. What that means to companies is that you've got to make sure not only that you protect the firewalls that keep people out who aren't supposed to be in your systems, but also that you have internal systems that will monitor the actions of your own employees and cut short any bad activity on their part.



Cyber Threats

- Insiders
- Hackers
- Virus Writers
- Criminal Groups
- Terrorists
- Foreign Intelligence Services
- Information Warfare

Figure 4

The reason why insiders are first (or in this case the least serious) on that list is that, other than in a critical company or infrastructure, insiders don't generally pose quite the national security threat that is the focus of the NIPC charter. They sure present a financial threat and a company threat. Depending on the company, that could be a national security issue, but from the standpoint of the way the NIPC looks at cyber threats, that's often only a company problem.

Then you go to hackers and so forth. They keep getting worse and worse, not in terms of the damage they can cause in terms of money but in terms of the damage they can cause to national security. Hackers and virus writers are the two that we read about all the time: Code Red leads one to NIMDA, and on and on. They come from virus writers and hackers.

You have seen little on criminal groups, and nothing on terrorists or on the last two, but those are the most serious. When we look at NIPC as a center, we have been in the business of dealing with the top end, because that's where our communications with the public are focused most often: we have to try to deal with the health of our networks. But the bottom end, information warfare in particular, is what we ultimately need to work against, and there is no experience on information warfare and not much on foreign intelligence services. So you have to keep in mind that it's like weapons of mass destruction: you have to worry about the soldier with the rifle, but what you're really worried about is that nuclear bomb and its delivery. That's kind of a comparison with this list.

We've seen a lot of work with criminal groups—in particular, as I was mentioning earlier, criminal groups out of Eastern Europe, the former Soviet Union, Russia, and Ukraine. There are a lot of groups that have been pretty persistent in going into credit card records from financial institutions and then trying to extort money from those institutions. That's basically a criminal matter. When the NIPC about a year and a half ago put out warnings about this kind of activity by criminal groups, it really didn't receive much press or recognition. Then we saw more and more of it taking place. Finally we thought we needed to hold a press conference about it to get the message out that there are groups trying to do these things and they have been successful, so you need to look at your systems.

I can tell you that's still happening today. Many times the way it happens is when you let others do what is not your core business. When we talk about insiders, let me add the word "outsourcing." Today you've got insiders you didn't know you had, and those happen to be outsourced contracting organizations. There was just something in the paper this morning about a leading company in the domain server business that was contracting out some of its work. The company was doing what many other companies do in the services business. You come in and say, "I'm going to sign you up to perform this service," and then you leave and, as with your mortgage, you assume that's who's doing your work. Yes, they're the ones responsible, but they may not be the ones doing the work. They hire another company in Jacksonville or wherever to do that piece, and that company is not as strong from an information assurance or protection standpoint. All of a sudden, if your server happens to be handled by this company, you get hacked, which is what happened yesterday and was reported. Company Web sites were being defaced; I think it was a Brazilian group doing it. All of a sudden companies were going to the domain provider and saying, "How could that happen? Why did it happen to me and not to one of my competitors?" The answer was, "Because your Web site is being worked by *this* company." The companies said, "I never knew that. I thought you guys were doing all of it."

Contracting out is a big deal. It also relates to these criminal groups that were doing the credit card attacks. A lot of the banking database support has been contracted out to other firms, and a lot of times you say, "Do you have a history of this? Can you do this? What's the price? Okay, go ahead and do it." It's not, "How secure are you? What's your reputation for security? What do you have in place?" There's no other technical person who goes into those negotiations and asks those questions, and so the chief executive officer or the chief financial officer or the shop owner signs off, and all of a sudden you've got a Pinto instead of a Cadillac. You figure you're only a small business owner anyway, and it doesn't matter, but it does.

That's an issue we have, and I just wanted you to be aware of the soup-to-nuts kinds of things we have to do as an organization, and really are responsible for. Credibility is our most important product. We're going to talk a little more about that as we go along, because the Center's credibility for not sharing proprietary information with others, but sharing information that's important to everybody in a timely manner, is extremely important. When you have to go from the top level of threats on the slide all the way down to the bottom, there are a lot of issues, not only of need to know but also of security, that come into play when you start sharing sensitively derived information that other people need to know about. It's a fairly broad range of things.

Clemons: Sir, you talked about this a little at lunch, but maybe it's a good time for the rest of the class to hear it. Could you describe your roles with regard to identification and then response, taking criminal groups as an example? After the crime has been identified or suspected, what does the Center do, and how does it involve the FBI [Federal Bureau of Investigation] and other agencies for follow-through? I know you're adjunct to the FBI, but could you just walk through that scenario?

Plehal: I could take criminal groups or any of them, actually. A hacker can take your system down and cost you all kinds of money, just as a criminal group could. It's still a violation of federal law.

Basically, a company comes in and says it's been hacked into, or its Web server has been taken down, or it's gotten a virus, or it's been extorted, or whatever the situation is. More than likely a company reports it to their local law enforcement agency—normally the FBI, because it's a federal crime—or the local police. If the local police get word of it, they would then work with the local FBI to start an investigation on the problem.

I appreciate the question, because the NIPC is not a law enforcement organization. We'll get to that in a minute. The FBI, of course, is. The NIPC's purpose is to get information and disseminate information to others. Part of the information that the NIPC would be getting is "XYZ Company was hacked into and extorted on this particular thing." The NIPC's view is that we do not want to victimize the victim further. That means that if you, as the bank president, came in and said, "I was hacked into and extorted," the FBI office or the local police will not put up yellow tape around the building, seize all the computers in your bank, and haul them off for the next month so your bank can't function. If the company does not want any publicity (and of course financial services companies never want adverse publicity, because credibility is really what they're selling) we don't want to damage that. What we try to do is investigate, and the NIPC would actually coordinate the investigation. We say that we institute investigations, not prosecutions. We're looking to see how we can help this victim to get out of whatever has happened and prevent other companies or people from becoming victims.

So you have two things happening. You have an investigation that is taking place quietly, and you try to sanitize the information put out to the rest of the community, the rest of the sector, and the rest of the country, to say, "We have recently learned of a vulnerability in ABC," but you don't say that it's because XYZ Bank lost $50 million. Ultimately you may want to release some of that information about money or the way it was done to motivate companies actually to listen to what you are saying. But in the first instance you want to ensure that you don't further victimize the victim. You want to get to the perpetrator, figure out what the issue is and how that victim was victimized, and help to prevent others from being victimized in the same way.

Student: Can you comment on how well that process is working from the perspective of the Moonlight Maze investigation, which is perhaps a little closer to home for the DOD people here?

Plehal: I really can't on that one. It has been in the papers. Moonlight Maze was an investigation that took place regarding an entry into sensitive systems, not necessarily DOD systems. Some were universities doing DOD work. Universities and the DOD share much in many cases, but one thing they don't share is culture. Universities feel that anybody who's an academician should have information about anything there in the broadest sense of sharing thought and knowledge. That's the good thing about it. From the DOD's standpoint, they're very cloistered. It's a totally different culture. A lot of the intrusions into systems were into free systems in universities, many of which had DOD contracts for research. It was a very sophisticated entry.

Hackman:[5] If I'm a bank and something happens, I know that you guys live in the FBI building and you've got a lot of FBI guys on your staff, and I know what the FBI does. How do you get me to believe that you're not going to take my tapes? There's a lot of stuff on that tape that I really don't want getting out, partly for competitive reasons, but maybe partly because it gets a little close to what might not be legal for me to be doing. I know that the FBI does investigations with the intent to prosecute. So how do you convince me that you're my friend?

Plehal: Many times it takes your becoming a victim and deciding which is worse: being in the press for having lost all this information and credibility and whatever else or at some point sharing that information with government so that you can stop hemorrhaging. You've hit upon what is really the crux of the question.

The answer is twofold. We talked about it a little bit at lunch today. One is structure and two is credibility and performance. Structure goes to the Freedom of Information Act [FOIA] at one end. FOIA is a wonderful thing. Anybody can come in under FOIA and request information that's been given to government organizations, but there are some exceptions that allow the government to protect information it has received. NIPC feels that the FOIA is broad enough to protect private companies' information that is voluntarily shared with the government. Private companies don't think that FOIA goes far enough. Companies won't share if they think their information is not structurally protected. Maybe you can fix that with legislation. Basically, the first question is: "What information do you provide that is protected under FOIA legislation?" You don't want to have a court decide whether this piece of information is subject to a FOIA exemption, meaning the legislation is weak or unclear.

Second, then, is that from a structural ability to keep information secure you have to demonstrate a cultural ability to do so as well. You have to have a history, and you have to have the interpersonal relationships to say, "Look, you can share it with us. We will not divulge it. You're protected under FOIA." Then you have to live by that, and the first time that information gets out, even if it isn't your organization that has let it out, your credibility is going to suffer and people are not going to come forward voluntarily.

I was mentioning the example of Microsoft earlier. Microsoft is being sued by the Justice Department. Attorney General Reno started the suit. Microsoft is the biggest software maker and

[5] J. Richard Hackman, Cahners-Rabb professor of social and organizational psychology, Harvard University, attended Admiral Plehal's presentation.

as a result is responsible for the introduction of numerous vulnerabilities into our cyber infrastructure. So we as the Center go to another level of Microsoft to say, “You’ve got to tell us about your vulnerabilities. You’ve got to talk to us about your software. You’ve got to talk about the compromises.” We imagined that they must be thinking: “Whom do you work for?” “Well, we’re in the FBI.” “Who’s the director?” “He works for the attorney general.” “She’s over here suing us, and you want us to share this information with you?!” It’s a very tricky thing. Basically we’ve been able to work that out, even with Microsoft, but it isn’t easy, and it doesn’t come very fast.

Student: Sir, I could point out that you’re probably working with him already. Howard Schmidt, the chief of software security for Microsoft, is an Army reservist.

Plehal: Did you know that he gave up his Microsoft job? Howard Schmidt was the chief security officer for Microsoft, and he was the one we worked with on those kinds of things. He has taken a job as Richard Clarke’s deputy for critical infrastructure protection at the National Security Council. He is an Army reservist. After 9/11, he came on immediate active duty at JTF-CNO and at NIPC. We work with Howard all the time.

I think it goes even more to what Richard [Hackman] was talking about. What if we’re investigating, and all of a sudden we find that you’ve violated some laws? Now what do we do? Do we turn you in to the FBI to investigate? If we do, we’re toast. But if a wrongdoing comes to our attention, we may have additional legal responsibilities. Fortunately, we haven’t had to cross that bridge, but you can see how that would be a difficult problem.

Student: Do you see many challenges from members of Congress about protecting that information? It seems that some of them would have a problem with the idea that a financial institution could tell a government, taxpayer-supported agency but won’t tell its customers or a private entity that there is a problem. I was just wondering if you had debated that or addressed it.

Plehal: Oh, yes, and I’ve told Ron Dick, our director, who is an FBI agent. After I had been at NIPC for a few weeks I said, “You know, Ron, I’ve come to realize that you and I deal with five or six things in most days that could get both of us fired just for making wrong calls.” You’ve hit on one that goes exactly to what Richard was talking about: SEC [Securities and Exchange Commission] violations, or financial violations, where a company has not divulged something. It may have given a false statement to the media about something that was leaked somewhere and said, “No, we haven’t been hacked,” or “No, we haven’t lost money, or the identities of our customers,” and we know it has. Sometimes we know it has and the company doesn’t know we know it. In other words, the company hasn’t told us.

Suppose we’ve gone into an investigation and found a company that was hacked into and lost data. Now what do we do? Should we go to the company and say, “We know you’ve lost data and whatever else”? That’s one option. The other is that if there’s an item in the press and we’ve got hard evidence to the contrary, even though the company hasn’t trusted us to pass on information, should we tell the investigative authorities that this has happened? If that happens, does that affect our credibility, even though we didn’t promise not to tell? Would that affect our credibility to receive information from others? Of course it would. So the SEC is a big one.

These are just things we have to deal with daily. It gives you an idea of the difficulty of having a center that’s so engaged in all these areas with “What is the right thing to do?” We could go up to Congress and say, “Yes, we knew this other company had been hacked into. We knew they had lost these data.” “Aren’t you supposed to share with law enforcement?” “Yes, we are.” “Why didn’t you do it?” We’d look foolish. No matter what we’ve done, it appears wrong, for different reasons. In the end, full disclosure is always the best policy and we encourage victims to be forthright with the public. As a center and a government body we strictly meet our obligations, while allowing the victim the ability to manage the incident forthrightly.

Hackman: Just to follow up, there’s a parallel in aviation called the Aviation Safety Reporting System (ASRS). If you’re a pilot and you’ve blown an altitude or something and you’ve turned that in, you get some immunity because it contributes to building a database that will make everybody safer. The cost-benefit analysis clearly is in the direction of reporting that rather than keeping it secret. Do you think you could get the legislation or whatever you would need to be able to provide that level of protection? What you’ve got to do is develop a track record and never slip once, because one slip on this and you’re completely dead. They kind of walled off the ASRS and it’s never slipped. It has a wonderful reputation, and people tell them stuff that they ought to tell them that could get them fired.

Plehal: We’ve talked about that. That’s a great example. The difficulty is that it allows somebody to come forward and give information voluntarily. What if you have a case where there are criminals over there in this bank and they haven’t told anybody the truth? You can snitch on them, and it’s almost the same. That’s hard to do, because then it’s, “Well, you reported on these people.” We could say, “Maybe if you’d reported to us earlier, we would not have reported you.” How does that work? It’s a real conundrum, I think. It’s just going to have to be worked out.

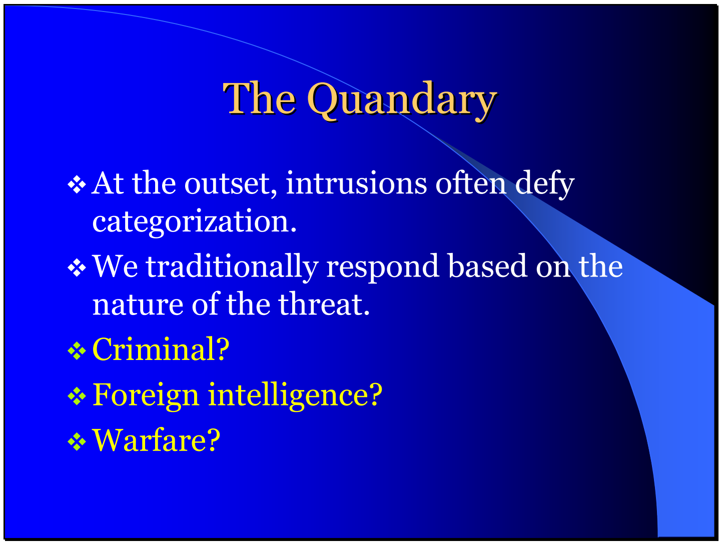
Student: Another follow-up: If there were no NIPC, would these companies in the private sector develop their own secure systems? Is there a national security benefit that outweighs sharing information? Obviously, it’s a balancing act. What’s the exact rationale for the Center? Let’s say a financial institution was hacked into and you found out that it was withholding information from the public. What is the rationale for not sharing? You can take that information and share it with other companies around the nation privately, without saying whom you got if from, just to learn how the hackers are behaving.

Plehal: The purpose of sharing is to identify vulnerabilities. It’s to figure out techniques and tools that hackers or criminals may use. It’s to share best practices with companies so that they can protect themselves from these same kinds of entrances and victimizations. So it helps the sector. Most of these things are not sector-specific; they are infrastructure- or IT [information technology]-specific, or they apply across the board. So they’re worth sharing with everybody, and that’s the purpose.

A company does not need the NIPC to have a secured system. The company can do that on its own, but the idea is that not everybody is going to do it.

Let me use a highway analogy, or cars. A car has to meet certain safety standards, and if it doesn’t have good brakes or whatever it could kill people. The thing is that it kills people on one part of I-70, and three or four people die. If a system that everybody is connected to is not safe, then everybody may be vulnerable. That’s part of the problem with the interconnection on cyber. It’s not quite like safety in cars, and yet we have much stronger safety legislation for autos than we do for cyberspace.

This is really the core of the problem (**Figure 5**). At the outset, intrusions defy categorization. When you have an intrusion, you don't know who is doing it, or where he/she/they is/are or even if the intrusion is in one place, or what the motivation is. All three of those questions need to be answered to figure out how to respond in a punitive way, in a sense, or in a protective way. So, if it turns out it's a foreign state messing with anything—it doesn't have to be a government system, it could be a company or anything else—as you know, we've got many ways that we as a nation can respond. We can respond economically, diplomatically, even militarily. We can bring in the press.



The Quandary

- At the outset, intrusions often defy categorization.
- We traditionally respond based on the nature of the threat.
- Criminal?
- Foreign intelligence?
- Warfare?

Figure 5

The response is dictated by who's doing it and what their purpose is. When there's a hack or an entry into a system or a defacement of Web pages or, worse, a virus, first of all, what is the impact on everybody? Is this thing going to stay focused on this particular node, or is it going to spread like crazy across the Internet? How is it going to be contained? What are the tools? We need to know the technical side of it. But ultimately the interest is in who's doing it, where they're doing it from, how they're doing it, and then what the motivation is.

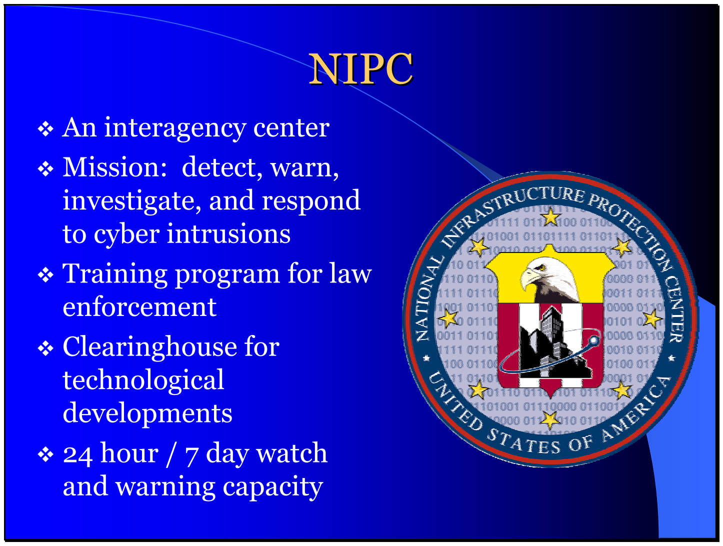
This gets you to why the NIPC is in fact located in the FBI building. It is because almost everything that happens via cyber that affects us somewhere comes through either the victim, because the victim is usually in the United States, or a "U.S. person," according to our definitions. If it's a U.S. person, can you use intelligence authorities to investigate? The answer generally is no. You have to use criminal authorities. So the FBI is really the only agency that has the federal criminal authorities. You don't want the NSA going after U.S. persons to figure out what's happened in a particular network. You don't want the DOD going into some U.S. person's mailbox and looking at that person's machines, unless we're talking about a DOD person. So criminal authorities are the authorities that are used to launch most investigations. That's the main point I want you to understand.

Whenever there’s an incident, an investigation is started. This investigation is not started for the purpose of ultimately putting somebody in jail. You may not ever want to put the person who did this in jail. You may want to do something far worse, depending on where the actor is and what the motivation is. The criminal authority gets you in the door to look at the system.

Now, a number of cases have moved from criminal to foreign counterintelligence authorities, if in fact the perpetrator appears to be entering into a system for foreign intelligence purposes. Then you shift and you get into the Foreign Intelligence Surveillance Act and the different legal authorizations. You can start using the most likely cases. The FBI has foreign counterintelligence authorities, as do the Central Intelligence Agency [CIA], of course, and others, depending on where the person happens to be and where the trail leads.

Finally, if it’s warfare, you move to yet another title, particularly in the era when we’re talking about computer network attack. You want to fry somebody’s system, or you want to take somebody’s power grid down, or you want to strip somebody’s banking system. The decision that it’s a foreign state is made by the president. It’s very important to find out where that person is so that you can use the proper legal authorities to continue the investigation on that person, but almost always the investigations start as criminal investigations.

The mission of the NIPC is to detect, deter, assess, warn of, respond to, investigate, and help mitigate physical and cyber attacks on the nation’s critical infrastructures (**Figure 6**). As I mentioned earlier, our main focus has been on cyber. We have a training program for federal, state, and local U.S. law enforcement and foreign law enforcement. We do train foreign law enforcement organizations in cyber investigations. We’re also a clearinghouse for technological developments, and we do have a watch, twenty-four hours a day, seven days a week. The idea is to warn of cyber incidents that the public needs to be aware of.



NIPC

- An interagency center
- Mission: detect, warn, investigate, and respond to cyber intrusions
- Training program for law enforcement
- Clearinghouse for technological developments
- 24 hour / 7 day watch and warning capacity

NATIONAL INFRASTRUCTURE PROTECTION CENTER
UNITED STATES OF AMERICA

Figure 6

Even this sounds pretty simple. When somebody has hacked into something, we put out a sanitized warning, and that’s it. Most people don’t read our warnings, and sometimes we have to go to the press and turn up the volume. Our director talks about this. Rather than putting out a written note on our homepage, or just sending it around, we also need to tell the press.

That's what we did in what was called the Card Keeper case that I mentioned: all those credit cards that were stolen from Eastern Europe. We also did it for Code Red. If you remember last summer, this was a really big deal where we went out and warned the public. You may not have paid too much attention at the time, but it was fairly significant. Not only did we have regular press conferences to update the tracking on Code Red, but we also weren't alone in doing it. We had the DOD, we had the private sector, we had the FedCIRC [Federal Computer Incident Response Center], and a lot of other organizations there. We were standing out in front of the American public, saying, "We are all looking out for our cyber health and welfare as a nation. It's not just the NIPC; it's all of us, and we're working together to face this thing and identify it." That's how we did it.

Student: In terms of the scope, even though it's an interagency center, the mission statement looks very much like the old FBI model: detecting something that has or has not been warned about and investigating it. It's very plainly a reaction-based mission statement. Do the NIPC's objectives include getting out in front, and trying to identify the people who might be responsible for doing something in the future?

Plehal: I mentioned a few extra words that weren't there. "Deter" was one of them. That also maybe doesn't look quite as proactive as it is. To deter, you have to be proactive. But the "warn" piece is where it's a twenty-four-hour watch-and-warning kind of thing. If we see something coming, we're going to warn ahead of time, and that is certainly a proactive piece. That can go very specifically to a particular incident or a particular vulnerability.

"Protect" is another word that isn't in the mission statement, but it's in the name of the Center, and it's there in the longer mission statement.

Student: Is "preempt" in there?

Plehal: No, it's not.

Student: Should it be?

Plehal: I think "deter" includes some of "preempt." The NIPC is not going to be an active defense organization in the way the DOD is. In other words, in an active defense organization, if you know a particular computer is going to send in a bunch of packets to deface your Web site or send you a virus at eleven o'clock, you can go into that computer and fry it at ten o'clock. At this point we're saying that's not our charter. We try to identify the threat. If it's a foreign counterintelligence or a foreign power threat then we would hand that to the DOD to execute or to fry that computer, if they saw fit to do so. If it's a hacker, law enforcement might seize the criminal's machine. That's the other part of preemption. There's the deter part, and there's the making sure it doesn't happen part. We're not in that wedge.

Student: Can you work through ISPs (Internet service providers) to help with this?

Plehal: Absolutely. The ISPs have been kind of dragged into this, and are finding out that they need us just as we need them. Code Red and NIMDA were good examples where the ISPs were saying, "Okay, there's more traffic on the Net. We get paid on traffic, and it's not our concern."

But some of the more serious worms and viruses were starting to come along, and they saw what kind of payloads those things carried. If they bring down the Net, then the ISPs are not getting any revenues. So the backbone providers in the first instance, and then the ISPs afterwards, have been on board working with us the whole time, and are more and more becoming believers, because it's the health of their networks that gives them their revenues. If it's a major backbone provider and everybody's down, it hurts everybody.

Hackman: Why did you say earlier that they don't read your warnings? If I were a manager of a major network I would have it in my bedroom.

Plehal: You might, and Howard Schmidt at Microsoft might, but, again, most companies look at IT as an enabler for business. It's something that you pay money for. You don't earn money from your IT protection. That costs you money. It's only when you lose it that you realize it's important to the bottom line. Most network administrators are not professional security administrators. The big companies can maybe afford it, but then you have all the mom-and-pops out there whose thirteen-year-old kids are running their net.

Hackman: Do you work through the CERT [computer emergency response team]?

Plehal: Yes. CERTs are interesting things that we can talk about. There is a bunch of CERTs around the world. Our CERT is at Carnegie Mellon University in Pittsburgh. It's the one contracted by the government to get intrusion information from the private sector. Many times companies are willing to talk to them, and they can talk to us, so we don't get involved in what the company is and what its particular issues are. The CERT is kind of a filter for companies.

The good thing about the CERTs is that there is that disconnect from government. The bad thing is the disconnect from government, in the sense that the CERTs are not all collecting all the information in the same way, and that needs to happen to allow us to better analyze the threats and some of the vulnerabilities that we have. But the CERTs are a very important piece. I think we're going to be helping more to drive what the CERTs do, based on what we need to do the analysis.

Clemons: I think this results from the notion that you can only stand on your toes for so long. I was reading an article recently in either *Newsweek* or *Time* that said that Governor Ridge and Homeland Security had decided that they were going to start color-coding the warnings, and the question they asked was "Does that make you feel more secure?" Actually, only 17 percent felt more secure. I don't know if that means that 83 percent didn't, but even in a relatively small, garrison organization there are literally hundreds of warnings with no color coding, if you will.

I agree with you; there's room for NIPC to understand the functionality and end result and the response piece, and maybe a bit of the deter piece, and to grab that and structure it internationally as well as nationally. This is just as a free thought here. I'm not offering a solution yet, but I think that trying to rope together all the disparate methods and reporting structures, and even what's reported, could be a real boon for understanding it and then moving to figure out some warning system that's maybe not color coding, but that allows the private sector to come off its tiptoes.

Plehal: That's right. It makes you think a lot. There was a lot of fun made of the color coding, and I can see why. Frankly, I don't feel more secure seeing a bunch of soldiers with M-16s in airports either, particularly when I've been in an airport that's been locked down because somebody ran through the gate. They can evacuate the airport without guns.

We can make fun of these guys and the systems, but they grew out of the time when the FBI kept sending out warnings about bridges in California maybe being blown up. It's one of those "damned if you do, damned if you don't" situations. You only get so much intelligence. It's not like you can make up stuff to make a more valid case for warning. If you get information that somebody who has connections with so-and-so was looking at disrupting the grid or blowing up a bridge in California on Labor Day weekend, you pass that on, even though you don't think it's fully credible, because what would happen if it does in fact take place? There's not only the tragedy, but also how you are going to answer that in Congress. But if you do it, and nothing happens, people say, "Oh, those alarmists!" The trick with intelligence information, as always, is to match appropriate action to the credibility and specificity of the information.

I haven't heard anybody who's criticized the color system come up with a better idea. I'm not a fan of the color coding, although it's no different than Alpha Bravo Charlie for the DOD. So why is everybody dissing this? Who's got a great idea? You're king for a day; you're Governor Ridge. What system would you put in place?

I just came back from Singapore and Japan, where we had some international meetings. The countries in Asia have a regional CERT. Part of my point to the conference was that we as nations are relying too much on these CERTs as independent operations. They fulfill a function, and it's an important one, but we need to be driving more of the information they get and standardizing it. We have the one Net, so why shouldn't we have one system for collecting data, and maybe several ways of analyzing it? We need to pull that together.

CERTs are not going to protect us. They're information collectors. The CERT in Pittsburgh has great technical people who have been working on some of the vulnerabilities that we have. We hope they're always going to be there, and they do great work, and they do some dissemination, but they're not charged by the government with protecting our infrastructure. They're beyond an academic organization by far in that they are very operational, but what responsibility do they have to protect us? They don't have any. The government has that requirement.

The NIPC is hosted by the FBI. I mentioned why: because the FBI has both criminal and counterintelligence authorities. There are fifty-six FBI field offices throughout the country. In each field office they have a National Infrastructure Protection and Computer Intrusion Program, or critical infrastructure protection agents who can work these issues. Sixteen of them are bulked up: there are seven, eight, or nine people in the squads. Others maybe just have one or two, or they share. That's the investigative piece that I was talking about. The forty-some legal attachés, or legats, throughout the world work with foreign governments on investigations in those countries.

The Leaves[6] investigation was a good case in point. The Leaves investigation was about a pretty bad worm that was out in the wild. We weren't sure what the person's motivations were.

[6] Also known as the W32-Leave.worm. It attacked personal computers running the Windows operating system; it did not affect servers.

We were very concerned, because it looked as though the hacker had fairly major capabilities to attack the Internet as a whole, not just individual machines. We found out it was a twenty-four-year-old stock boy in a grocery store in London, England, who just had a lot of time on his hands, and he put this thing together. It was an amazing piece of work for a young fellow on his own. We worked with the legal attaché in London and brought him in. He was arrested, and that was a good collaborative case.

In the case of the Eastern Europeans, we did entice several members of this criminal hacker group that was taking credit cards into this country, and they've been arrested. I think there was one in Seattle and one in Boston. Again, there was a way to lure them into the country, and that was successful. I remember I was in a meeting where one of the people was deriding the NIPC, saying, "All you guys care about are investigations and prosecutions. You're never going to get these guys over here. They're in Eastern Europe." I didn't say anything, but we got two of them. There were actually three from Ukraine. Maybe it sends a message to our criminal groups, as well as others. The other piece is that we have to get a structure internationally so that the laws are the same, and we can prosecute them over there too.

Clemons: Did you broach the extradition element of it, or similar prosecutions, with Japan and Singapore? Is there an international agreement on how that would be done?

Plehal: First of all, it goes back to structure. The country has to have laws. Remember the I Love You bug in the Philippines? There were no Philippine laws that said you shouldn't do Love Bug kinds of things. So even if you get the person, how do they extradite him if they don't have a law that refers to it? The Philippines just passed that. The Council of Europe has been working those issues on the European side so countries would have similar levels of law. They could prosecute for themselves, but also allow extradition under those terms.

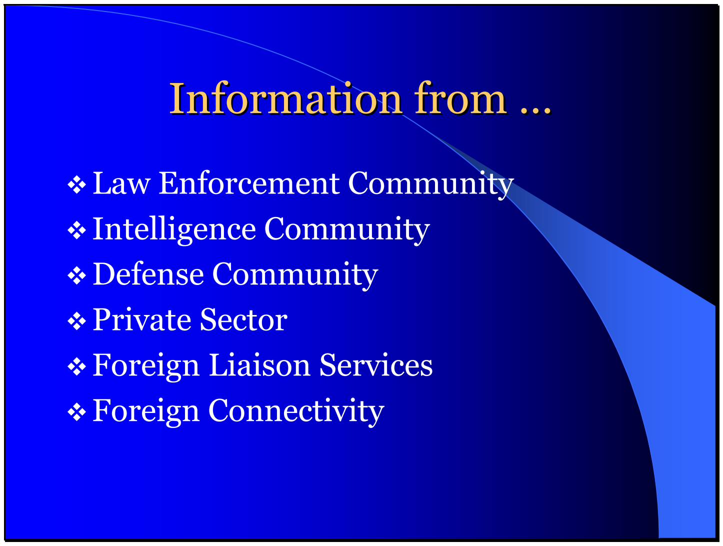
Australia, Hong Kong, Japan, and Singapore were the four countries at the meeting hosted by Singapore a couple of weeks ago. Their laws are not all consistent, but they're close enough to deal with most of the issues we had. So I think that's working pretty well with our major allies. We want to work with those nations that want to participate in the cyber business, such as Hong Kong. They're under the government of China, but they're still separate. They're very proactive in wanting to be leaders in the cyber area, so they have laws in place to deal with that. Countries that are talking to each other are not the problem. It's all the other countries that are the bigger problems: the former Philippines of the world, if you will.

Clemons: I guess I'm thinking of the asymmetric threat, and following that DOD paradigm. You talk about the European Union; it makes sense that they would build consensus on how to deal with the asymmetric adversary out there. I wonder if Afghanistan or the Taliban had an agreement by law about what they would do about extradition.

Plehal: You've got to have a government to have an agreement like that, and Somalia and Afghanistan don't. But out of the 200 countries or so, there are only about 40 that have really thought about and legislated much of anything in the cyber area. Certainly they're the major countries, but with a computer and an Internet, even if there's only one connection in the country, a pretty good hacker on it could cause a lot of damage, and the government doesn't care at all, because it isn't dependent on the infrastructure in the first place. But it's something that everybody's talking about. We're holding international meetings just to address those kinds of things.

The recent Bloomberg case involved Michael Bloomberg, who's now the mayor of New York. His company had an intrusion, and he was being extorted for many millions. The FBI worked it and it turned out the people were operating out of part of the former Soviet Union. They were lured to London to meet with one of Bloomberg's representatives to arrange payment, and were arrested when they got to London. Again, he cooperated fully and was involved with law enforcement, and we kept it well under wraps until they were actually taken into custody in London. So it really can work, and these are the kinds of successes that I hope will send good messages to industry that we mean business and that it is in the interest of the company to make it work.

We get important information from law enforcement (**Figure 7**). You can read the others. The private sector is key, and we've talked about that already today. As far as I know, the NIPC is the only organization in the government that has the legal authority and operational capabilities to do all of these things. That's very unusual.



Information from ...

- Law Enforcement Community
- Intelligence Community
- Defense Community
- Private Sector
- Foreign Liaison Services
- Foreign Connectivity

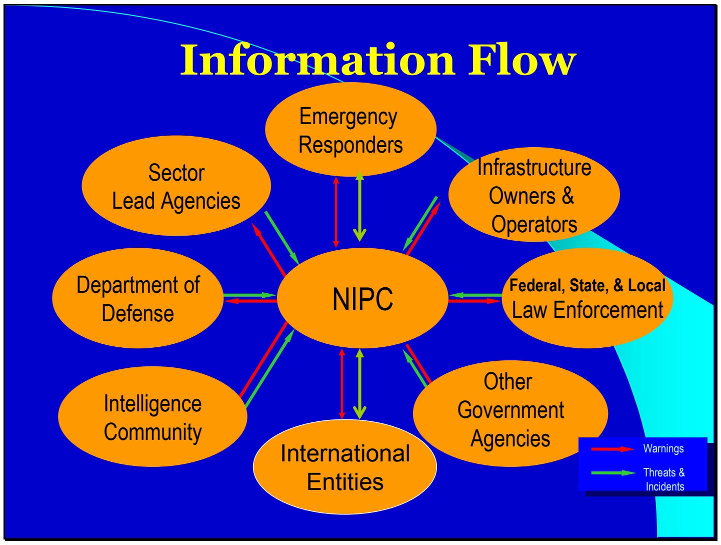
Figure 7

The solutions are a public–public partnership and a public–private partnership. The public–public means that the government is supposed to work with the government. Everybody knows that's easy to do, so the hard part is the public–private. Not really! Of course the personal interaction is where it must start. We have a law enforcement culture that says, "You do not share anything about a case with anybody, because it will undermine the prosecution." We have the intelligence community that says, "We don't share anything." It's not very easy to cross these lines. We all know that CIA and NSA can be at odds. They all have their own cultures that are very important to the professionalization of their particular organization and make them successful, but the culture also prevents information sharing across organizations.

There are some organizations within the government that until now haven't seen the need or been required to interact with others. Then there are agencies that have found new organizations with which they need to work in today's environment. The Department of the Interior, for example: should it have to work with the intelligence community or with the FBI? Generally there isn't a history of a need for Interior to work with these other agencies. It's a new thing for everyone.

The other one, public–private, we've talked about some today. How do we get information from the public, because that's where most of the information is that we'll be dealing with in the future, and share it with others in a way that doesn't violate a trust and reveal where it came from?

This is a slide that was put together more recently (**Figure 8**). Of course, the NIPC is at the center. In fact, it is a pretty accurate depiction. What you have is information sharing going back and forth as well as threats and warnings going back and forth, so it's kind of a hub-and-spoke arrangement. You could draw in all the other lines, but some aren't very mature. If you take the DOD, for instance, it has long-standing relationships with ministries of defense of many nations, particularly, of course, those of our closest allies. So there's better sharing between the DOD in this country and a foreign ministry of defense than there is between the U.S. DOD and maybe another U.S. agency. It's interesting that in the intelligence community, the defense community, and the law enforcement community, you have really strong links to the international communities, which in many cases are very mature and very robust. What we have to do in the Center is make sure we don't screw up those existing relationships, and at the same time bring everybody together in sharing information that should be shared.



Information Flow

Emergency Responders

Sector Lead Agencies

Infrastructure Owners & Operators

Department of Defense

NIPC

Federal, State, & Local Law Enforcement

Intelligence Community

International Entities

Other Government Agencies

Warnings

Threats & Incidents

Figure 8

I'll give you an example. When we were in Japan, we were talking about information sharing. Japan does not have a NIPC organization, although the national police is taking the ball and running with it there. It would be like the FBI standing up a NIPC. The FBI didn't stand it up in this country, but the national police in Japan are standing up a cyber protection center that is focused on law enforcement. I'm not a Japan expert, but the Japanese national police and the Japanese defense department are not any better than we are at sharing information across the communities. In fact, they have less of an infrastructure in place to share across.

We had our five-nation meeting, and then we had just a bilateral with Japan afterwards in Tokyo on our way back. There is a certain jealousy over the information that each has, and is entitled to, and how they share it, just as there is in our country. But you can envision a situation where the NIPC comes into information that has to do with a threat on the defense side, so we're sharing that with the DOD. The DOD is going to share that with the Ministry of Defense in Japan. Now, at the same time, the NIPC is sharing with the national police in Japan and their organization. Let's say we share with them fairly early, and the DOD has not yet shared with the Ministry of Defense, so this ministry does not yet know of the issue, because the national police doesn't pass it on. What if the Defense Ministry turns to the DOD and asks, "U.S. DOD, why didn't you tell us? We thought we were a valued partner in this, and here our national police have known all about this for a week, and you haven't shared it with us." These are really very difficult things that we're going to have to deal with.

My point to the Japanese government was, first of all, that they can't rely entirely on their CERT. Second, we can't tell them how to do business, but for them to be as effective as they need to be in their nation they need to have a NIPC-like structure, so that if we share information with them on cyber things we can be sure it gets to their Ministry of Defense, commerce folks, and banking sector, because we're counting on them to pass the word. At the same time, we're counting on them to pass information to us that is going to be important to all of us in our structure. So it's a difficult issue, because the national structures are not parallel.

We had a recent case with the Canadians that made us look pretty bad, because Canada does not have a NIPC. They have what is called OCIPEP [Office of Critical Infrastructure Protection and Emergency Preparedness]. When the NIPC was stood up, people thought that it was not going to work, because it was in the FBI, and some people distrusted the FBI. They were waiting for it to fail. They said, "To be effective, it really needs to be in the DOD." The Canadians heard this, and they decided not to put their OCIPEP in the RCMP [Royal Canadian Mounted Police]. They have theirs more defense-oriented, so it's in a different structure than ours. The Australians and the Brits have a different structure, so everybody's kind of looking at it differently.

The point is that we've got to get to a situation where we can all share government-to-government, and we didn't share with the Canadians. The OCIPEP did not have the same watch-and-warning capability that we do, so they did not get the information on a recent incident, and were not happy with us for not having shared it with them. In fact, we did share it, but it was through a channel that just wasn't working well in their country. We really did try, but they don't have the same infrastructure to receive our information. We're still working to make that better.

We have to change this a little bit when it comes to homeland security, because there's a need for state and local protection. We have no way, other than through law enforcement, of sharing information with state and local governments in this country. We don't share intelligence or DOD information with state and local governments. There is no mechanism. So here we are potentially in a situation of sharing information with foreign partners that we're not even sharing with our governors here.

So we've got a lot of infrastructure to start working on, not just for homeland security and antiterrorism, but also for foreign power issues and others that are certainly related to the cyber business. We've really got a lot of work to do in trying to put some of these things together so we can have a robust sharing structure. The Governor Gray Davis warning on the bridges just took a phone call, but ultimately, when you have routine threat information or actionable intelligence that needs to be worked on by state and local governments to protect their own companies, states, or infrastructures, we need to have a system in place. Today it is very tenuous.

Clemons: How would you characterize the state and local governments' desire for it? Increasing, I would hope. Do you see a bunch of "SIPCs" [State Infrastructure Protection Centers]? Taking the Japanese model you spoke about, and their need to set up a NIPC or a "JIPC" [Japanese Infrastructure Protection Center], is that going to be replicated in state houses?

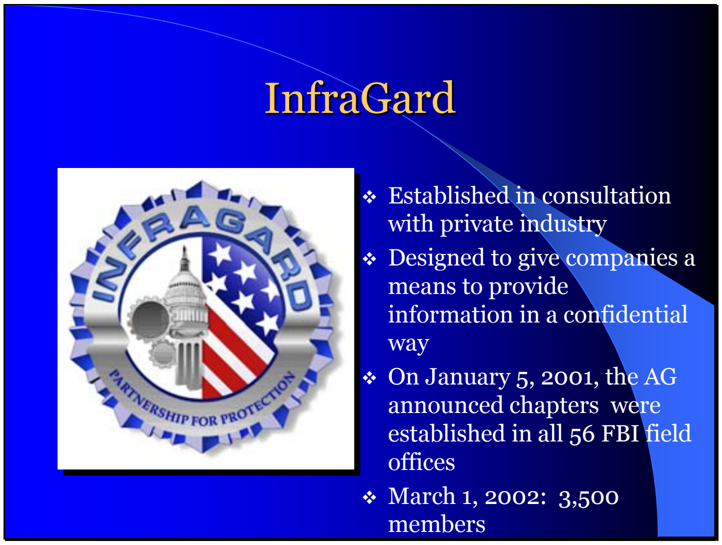
Plehal: It could be. But then the states have to use their authorities to set up capabilities to receive the various types of information, and they have to know how, so it would be a totally different way of doing business for the states. When the president wanted to call the governor of Maryland after September 11 on an issue regarding protection of assets in the state of Maryland, he said, "Get him on my classified line," and the governor said, "What's that?" The governor didn't have a STU [secure telephone unit]. That's been a big deal—a STU for all the governors. "Well, who's going to pay for them, and once they get them, how are they going to use them?" Anyone who's dealt with classified information knows there's a culture about protecting that information. You don't just hear something and pass it on. The state of Texas is very aggressive in this, as are Florida and New York. We could talk about this for a long time.

Clemons: There are a couple of papers in there. That would be a great topic.

Plehal: I've been talking too long. Let's page through a few more slides really quickly, and then go on to questions.

I skipped by public sector sharing. We talked a bit about that, but there are a couple of things I want to mention about how we share information with the public in this country, without the state and local things that we talked about.

InfraGard is a program that grew up out of the Cleveland field office of the FBI (**Figure 9**). InfraGard is an FBI-encouraged program. It's a horizontal sharing of information and need. For example, Boston has power companies, water companies, manufacturers, IT companies, telecommunication companies, banking and finance, oil and gas, et cetera. They're part of different industries, but they all have similar concerns: "Where am I getting my power? Is it secure? Where am I getting my water? Is it secure? Where am I getting my food, my telecommunications?" So, an InfraGard chapter in Boston (there is one here, and it's free) is joined by mom-and-pops all the way up to Fortune 500 companies. They have their own local board, and what they discuss in monthly meetings—they bring in speakers, they host seminars—is the infrastructure within the area where they live. "What is our infrastructure? How is it interconnected? How is it protected? What are our needs as a community?" It's a very positive program, and there are about 3,500 members. They have a national board, too, where they elect their own people.



InfraGard

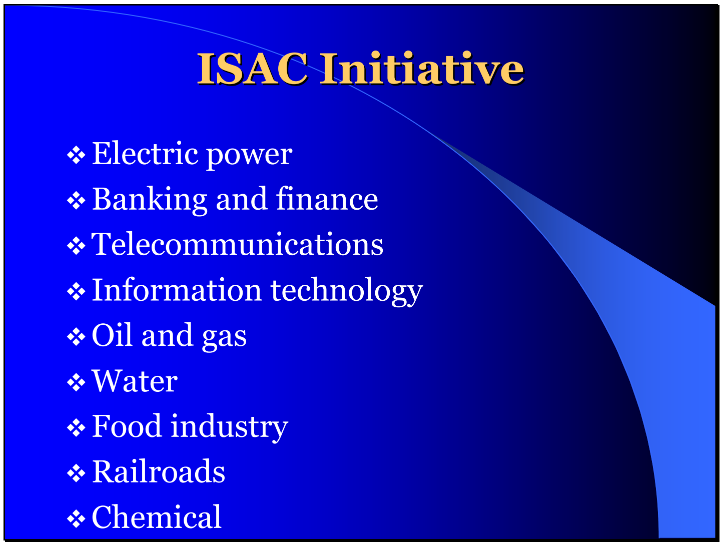
- Established in consultation with private industry
- Designed to give companies a means to provide information in a confidential way
- On January 5, 2001, the AG announced chapters were established in all 56 FBI field offices
- March 1, 2002: 3,500 members

INFRAGARD
PARTNERSHIP FOR PROTECTION

Figure 9

We communicate with the InfraGard membership. If you're an InfraGard member, you can ask to be screened by the FBI, and you can be what is called a secure InfraGard member. That means that members would trust each other enough to share their business-sensitive information. We have to be very careful that we don't create a bunch of different tiers of organizations in terms of whom we share with and who gets it first. As a public organization, we need to tell everybody who needs to get the information as quickly as we can. With the secure InfraGard membership we have a way of telling people things that may be more sensitive to the companies that provided the information for this purpose—things that we wouldn't tell the public quite as soon, and we can trust that they're not going to do something to counter the benefit of telling others later on, especially as we develop more information. We also can see if InfraGard members might be able to validate information that we are analyzing, so that we can give more definitive information to the public at large.

The other mechanism is the ISAC [Information Sharing and Analysis Center] initiative. This is a vertical initiative as opposed to a horizontal initiative. This tells you that a particular sector needs an infrastructure guru. ISACs cost money. They are national sector relationship groups. The members are mostly large companies, and these are some of the areas that are looking at standing up, or have already stood up, ISACs (**Figure 10**). They have their own boards. Some of them have hired people to do watch and warning for them. They're based on the premise that we in the information business or in the banking and finance business have certain needs that other infrastructures may not. We have certain vulnerabilities or issues that other sectors do not. We need to pool our resources to work on those things. If the money transfer system has problems, it's going to affect all of us in the financial services business. It will affect our credibility, so we need to make sure that it's secure.

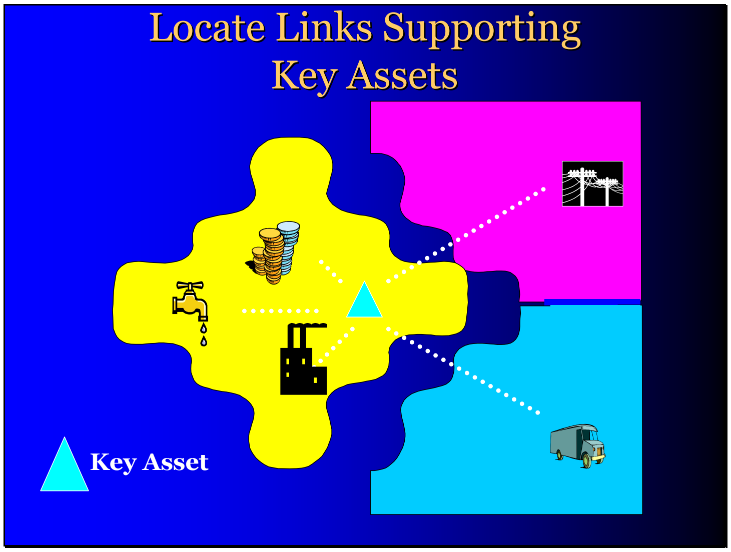


ISAC Initiative

- Electric power
- Banking and finance
- Telecommunications
- Information technology
- Oil and gas
- Water
- Food industry
- Railroads
- Chemical

Figure 10

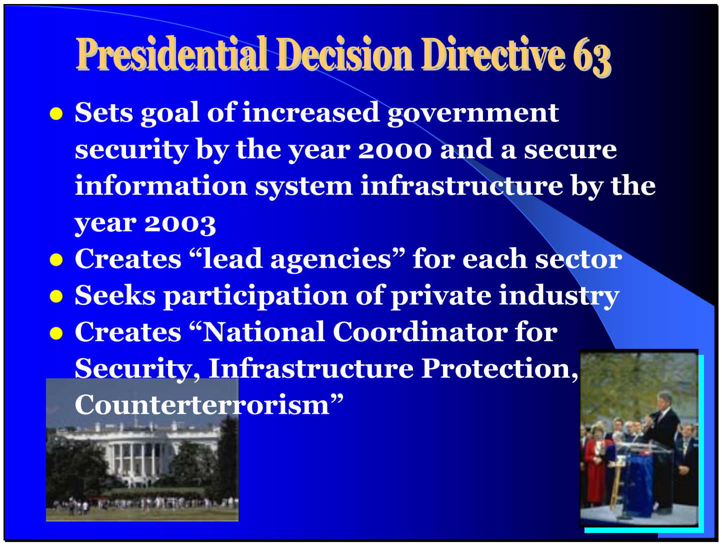
Another FBI initiative is called the Key Asset Initiative, where through the fifty-six FBI field offices and the legal attachés overseas we try to identify the infrastructures that are important to support the community that office is in (**Figure 11**). That again involves the same sectors, and it's an identification of the nodes and maybe the weak points in the system, so that law enforcement has an idea of what to protect in case of emergency, or what they might face if they were going to respond to an emergency in terms of critical infrastructure. The database exists. It's not a McDonalds french-fry database. Some offices have done really well with it, some haven't. From a national standpoint, we need to roll this up into a national key asset database. We've done some of that since 9/11.



Locate Links Supporting Key Assets

Figure 11

I have a little bit on PDD 63 (**Figure 12**), and I have a summary of the executive order that set up Governor Ridge's office (**Figure 13**). Homeland Security is terrorist focused, and Governor Ridge does not have an operational component. I think the word "coordinate" appears about forty-five times in the document, which means he doesn't have direct authority over operations. He just has to make sure that everybody else is doing what they're supposed to, and where there are no bridges he has to make sure they are created.



Presidential Decision Directive 63

- Sets goal of increased government security by the year 2000 and a secure information system infrastructure by the year 2003
- Creates "lead agencies" for each sector
- Seeks participation of private industry
- Creates "National Coordinator for Security, Infrastructure Protection, Counterterrorism"

Figure 12

Student: Tony is on record as saying some really pithy things about any mission statement that is based on "coordinate."

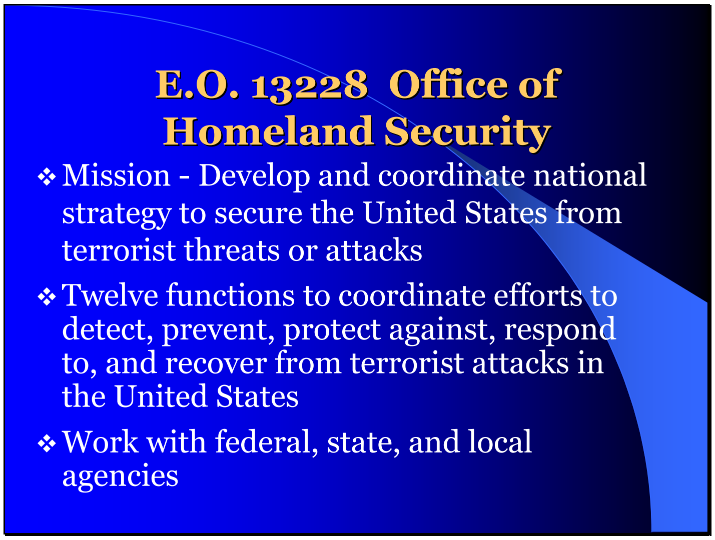
Plehal: He's right. Next, this is the executive order that set up the critical infrastructure needs in the information age (**Figure 14**), the one that Dick Clarke's committee has created. Fortunately, Dick Clarke has been doing this for several years, and so there is an operational component, if you will, and that really is the NIPC. Those two executive orders were signed out within a couple of weeks of each other, in October 2001. PDD 63 still exists. It did not get canceled by Executive Order 13231. That's part of the basis for this news article that was in the paper about Senator Grassley, because it's still in existence.[7]

Clemons: That was perfect. We have time for a couple of questions before you go.

Student: Sir, are you in D.C. yourself right now, on Pennsylvania Avenue?

Plehal: Yes. The NIPC is physically located at FBI headquarters, and we've got a lot of commuters.

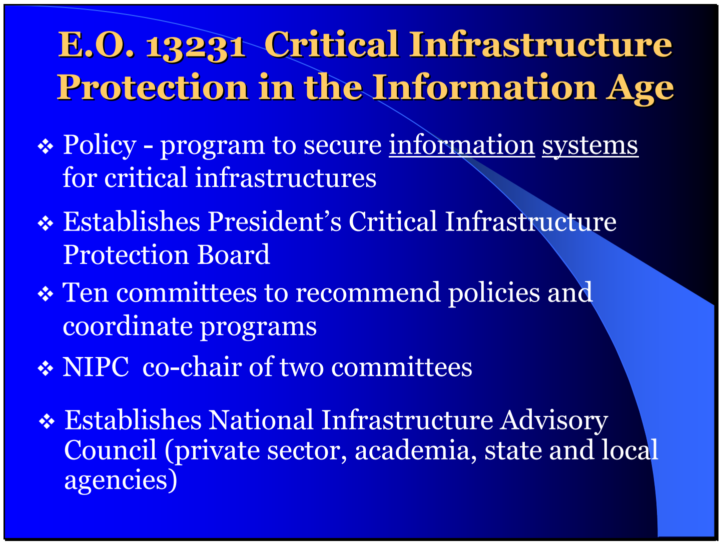
[7] See Joshua Dean, "Senator Urges FBI Not to Eliminate Computer Security Center," *Government Executive Magazine*, 21 March 2002 [On-line]. URL: http://www.govexec.com/dailyfed/0302/032102j1.htm (Accessed on 9 December 2003.)



E.O. 13228 Office of Homeland Security

- Mission - Develop and coordinate national strategy to secure the United States from terrorist threats or attacks
- Twelve functions to coordinate efforts to detect, prevent, protect against, respond to, and recover from terrorist attacks in the United States
- Work with federal, state, and local agencies

Figure 13



E.O. 13231 Critical Infrastructure Protection in the Information Age

- Policy - program to secure information systems for critical infrastructures
- Establishes President's Critical Infrastructure Protection Board
- Ten committees to recommend policies and coordinate programs
- NIPC co-chair of two committees
- Establishes National Infrastructure Advisory Council (private sector, academia, state and local agencies)

Figure 14

I will say that we've been running at about 105 or 110 people. We have a budget of about $19 million. We asked for a plus-up this last year of $40 million to get into the physical side of the business as well as some of the modeling of interdependencies—analysis that we need to do that we've just barely started. After September 11, we were given $60 million, which translated into additional people, about 328 total. We have space for 150, so we've now got a space problem.

I've enjoyed being in organizations that need to turn around if they're going to continue, and you don't know if they're going to be there. That's where NIPC was a year ago. Now it's much more robust, but managing and leading growth is an incredibly difficult thing. It needs different skills; it requires us to think about a lot of things, and basically we're trying to change the tires on an airplane while we're flying.

After the September 11 attacks, a lot of people were taken out of the Center and put into the FBI to support the investigation. We said, "Hey, we've got a center to run. We've got things we're still supposed to do. We don't know if we're going to have cyber attacks from whoever did this. We have to keep doing the mission." So we pulled some people back, but we were a skeleton crew for a long time. People started coming back, and then the DOD funded a healthy number of reservists (from all the services) to support us and to supplement the infrastructure side of the analysis equation, which has been a very significant addition.

During this period, the infrastructures have been calling in, wanting threat briefings. Once or twice a week they've been coming into the NIPC for briefings, so we've been doing those kinds of things. But in a 150-person center we're going to have 300 people, and that's a challenge in terms of growth: keeping people productive and focused, and growing the kinds of missions we can do. That's our current challenge.

Student: You've touched a couple of times now on your being primarily focused on the cyber threat. On the physical security aspects, could you sketch out what you see as the way ahead for the NIPC?

Plehal: Where we're starting are the physical components of cyber. That's one, and that's in the executive order. It's not too hard to get to that. If you've got a telecommunications node, and all the cables are running through a building in New York (which in fact was the case, and that building was close to being destroyed), how is that going to affect you in terms of the stock market and everything else? We're starting to analyze those pieces.

Beyond that, the sectors are saying, "Don't tell me that you're going to separate cyber and physical, because I've got SCADA [supervisory control and data acquisition] systems that are cyber, but they're connected to physical facilities, and if I lose them I'm in trouble." You can argue that's a physical piece of the cyber.

What's really happening now is that Governor Ridge is looking at physical counterterrorism kinds of things. Dick Clarke, under the other executive order, is looking at the physical pieces of cyber. They're both having committees meet like crazy about "How do we coordinate and do what's necessary?" Those two need to get together at the top. I'm going to meetings all the time, and they're the same kinds of meetings. One is for Ridge and one is for Clarke. We have to meld those much better.

Within the NIPC, what we've done is try to bring in infrastructure protection advocates from the different sectors. What do the railroads need from the Center? What kind of warning information; what kind of cyber information? We draw them in, and have them start driving our analytic group to say, "These are the products that this particular sector needs," so we have kind of a push–pull within the Center. That's what we're trying to create.

Student: The Joint Staff has an integrated vulnerability assessment team that actually works out of the Defense Threat Reduction Agency. Have you talked with them to see how they approach the business of assessing the vulnerabilities?

Plehal: Yes we have, but we're not really in the vulnerability assessment business per se. Sectors have to do those assessments. We're not trying to tell them that we'll come out and help them assess. We're going to try to implement best practices on cyber, but really the focus needs to be on: if there is information anywhere in the world that something might happen, we need to have it and then be able to pass it on to those who can take action.

Clemons: We need to get out of here, Sir, if you don't mind. To parrot Tony, we'd like to give you a small token of our great appreciation.

Plehal: Thank you very much.

Acronyms

ASRS	Aviation Safety Reporting System
CERT	computer emergency response team
CIA	Central Intelligence Agency
DOD	Department of Defense
FBI	Federal Bureau of Investigation
FOIA	Freedom of Information Act
ISAC	Information and Analysis Center
ISP	Internet service provider
IT	information technology
JTF-CNO	Joint Task Force-Computer Network Operations
NIPC	National Infrastructure Protection Center
NRSG	Naval Reserve Security Group
NSA	National Security Agency
NSGA	Naval Security Group Activity
OCIPEP	Office of Critical Infrastructure Protection and Emergency Preparedness (Canada)
PDD	Presidential Decision Directive
SEC	Securities and Exchange Commission
STU	secure telephone unit

Seminar 2002

ISBN 1-879716-81-X