*INCIDENTAL PAPER*

# Seminar on Intelligence, Command, and Control

**Infrastructure Protection and Assurance**
**Michelle K. Van Cleave**

**Guest Presentations, Spring 1999**
Charles J. Cunningham, Kawika Daguio, Patrick M. Hughes, Peter H. Daly, Walter Jajko, David J. Kelly, Gregory J. Rattray, Michelle K. Van Cleave, Robert T. Marsh, Randall M. Fort

**June 2000**

*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.





E-mail: pirp@deas.harvard.edu URL: http://www.pirp.harvard.edu
ISBN 1-879716-63-1 **I-00-2**

# Infrastructure Protection and Assurance

**Michelle K. Van Cleave**

*From May 1997 through December 1998, Michelle Van Cleave was staff director and chief counsel, U.S. Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information, chaired by Senator Jon Kyl (R-AZ). The subcommittee's jurisdiction encompasses law and policy for information warfare, counterterrorism, Y2K concerns, encryption, infrastructure protection, freedom of information, and export controls, as well as oversight of related activities by the Justice Department and the FBI. Ms. Van Cleave joined the subcommittee following four years Of Counsel to the Washington law firm of Feith & Zell, P.C., and consultant work for the CIA and Los Alamos National Laboratory. For a cumulative period of five years from 1987 through 1993, she held the positions of general counsel and assistant director for national security affairs in the White House Office of Science and Technology Policy; during 1989, she served as minority chief counsel to the Committee on Science, Space, and Technology, U.S. House of Representatives. From 1981 through 1987, Ms. Van Cleave was assistant for defense and foreign policy to Congressman Jack Kemp (R-NY), serving concurrently as national security assistant to the House Republican Conference and associate staff member, House Appropriations Subcommittee on Foreign Operations. She holds M.A. and B.A. degrees in international relations from the University of Southern California, and a J.D. from the U.S.C. School of Law. Ms. Van Cleave is a member of the bars of the State of California and the District of Columbia.*

**Oettinger:** You have read Michelle Van Cleave's biography, so you know her background. It has equipped her remarkably well for dealing with this seminar and the theme for this year on the overlap between what used to be civilian and what used to be military concerns, which now seem to get increasingly indistinguishable. However, she has had a number of different jobs between the time when she worked for Senator Kyl and now, so I would ask her to open up with a couple of remarks about where she's been and what she's doing, and then to lead us into a discussion of the civilian and the military in any proportion she deems sensible. It's all yours, Michelle. It's a pleasure.

**Van Cleave:** To respond to that last point first, what Tony is alluding to is that when I left the Judiciary Committee at the end of last year, I joined the office of the Senate parliamentarian for a brief period. We were talking about this over lunch. I was with that office during the impeachment proceedings against President Clinton. It was fascinating, and I enjoyed hearing all your views. But I was talking about the impeachment proceedings more at the anecdotal level.

Very recently, I left the parliamentarian's office to accept a position back in the private sector, with a small firm doing some defense consulting in areas that include our subject matter for today—infrastructure protection, or infrastructure assurance, take your pick. Does that respond to your request?

**Oettinger:** Yes, fine.

**Van Cleave:** I want to talk to you about some of my observations of the President's Commission on Critical Infrastructure Protection (PCCIP), which is the Marsh Commission. Tuck this away for your knowledge when General Marsh comes here to talk to you.

I've brought some slides to try to organize a discussion here about this subject, but let me just say this, so that we're clear on what we're concerned about. In national security policy, strategy, and decision making in the past, we very much had what I guess we would call the luxury of understanding what national security threats meant and who

was responsible for dealing with those threats within the context of the U.S. government. There has long been a lot of discussion on the general subject of economic security and the extent to which economic security and national security may be interdependent. The strength of one's economy will, in large part, sustain and support defense capabilities. These things are intertwined and long have been, but have also led to some very interesting policy discussions about what are sometimes seen as trade-offs; the area of export controls, for example, comes to mind. How far do you want to take prohibiting exports of certain sensitive or dual-use technologies in the name of national security, and how is that going to impact our economy if we're losing market share and profits coming back into the United States as a consequence? It's an example of the way in which these kinds of discussions or relative trade-offs have proceeded in the past. This has long been a part of our history and our concerns in national security.

What is becoming even more current today is an area that we in the United States have had little reason—some reason, but not great reason—to be concerned about in the past, and that is the point at which national security concerns leave off and domestic security concerns begin. What do I mean by that? This is an era where terrorist activities are increasingly of concern in the United States, and are crossing national boundaries. International terrorist organizations may involve participation or support by Americans, whether here or abroad, Therefore, domestic security and how you deal with the activities that may be taking place in the United States, be they fundraising or even operations in the United States, are interrelated with our international or national security concerns about these groups or entities abroad. How they cross our borders and how we deal with this interrelationship has become rather complicated. It's stressing for the institutions of government in the United States, because we have traditionally had a very fairly clear divide between those things that are national security and those things that are really law enforcement concerns.

Law enforcement concerns in the United States reside with the various law enforcement agencies—federal, state, and local—that have responsibility for keeping the peace. Their activities are circumscribed very carefully by the procedural guarantees inherent in the U.S. Constitution. They include such things as protection against unreasonable searches and seizures. The U.S. government undertakes not to collect intelligence per se on activities within the United States by U.S. citizens or by resident aliens. The Constitution forbids that sort of collection, unless there is a showing of probable cause that a particular individual may be engaged in behavior that may be unlawful. If a law enforcement agency can show to a court of jurisdiction probable cause for believing that a crime has been or is about to be committed, then the court will issue a warrant authorizing that agency to undertake the search or seizure incident to that probable cause showing.

If the issue is that we believe there is a threat abroad or an action by entities abroad that may threaten the peace here, or may threaten interests of the United States, the intelligence agencies of this country are authorized to collect intelligence on that activity so that government decision makers might understand what they're up against and act accordingly. There is no protection afforded to foreign entities against that kind of observation or intrusion. The Constitutional protections are domestic, not foreign, and the intelligence agencies are not circumscribed in the way that law enforcement is.

When issues arise that transcend borders, where the border distinction is not relevant, very serious institutional questions arise about who in the government is responsible for dealing with these things, and what rules of the road govern the way in which they may deal with these things. How can they work together if they need to share information?

This, perhaps, is very critically and clearly demonstrated in the area of information warfare (IW) threats to the United States and the whole cyberwar dimension. So much of what is involved in IW is really utterly irrelevant to any kind of sovereignty or borders, and it can be very unclear where a particular source may be emanating from. As a consequence, it has been very difficult for the U.S. government to get its arms around how to deal with this new category of threats presented to us.

What I would like to talk about today is the protection of the critical infrastructures of the United States against IW intrusions. Where we are, what the issues are, and how this has evolved are some things for you to think about as students of command and control matters, and what really is at stake in trying to develop a national strategy for protecting critical infrastructures. This is why I had hoped that Tom Marsh had already been here, because the PCCIP spent quite a long time looking at this issue.

**Oettinger:** Most of us have read the PCCIP report, or glanced at it. So we're in better shape than you might fear.

**Van Cleave:** Good. At this point then, let me show a few slides so I can talk from them. I think that there are some pretty basic questions here (figure 1), and the first one is: What do we mean by infrastructure protection or assurance? I put that up as the first question because it has been my observation in talking

- **What do we mean by infrastructure protection or assurance?**
- **What needs to be protected?**
- **Whom or what are we protecting it from?**
- **What are we assuring it to do?**
- **Who are "we"?**

**Figure 1**
**Basic Questions**

with different people who are involved with this subject that it's like the parable with the elephant: their definition depends on what part is closest to them, and what they grab hold of.

Since you've read the PCCIP report and (I hope) thought about this as a little bit of preparation for this class, I would like to throw out a question to you. What do *you* think is meant by infrastructure assurance or infrastructure protection? We should get some of those ideas on the table, and let's see if we still have the same view by the end of this discussion. Would anyone like to take a shot at that?

**Oettinger:** I'll point a finger if nobody volunteers.

**Student:** I'd say assurance would probably fall into the category of reasonable protection, in that you have some credible reliability of a system: when you turn it on, it will work.

**Van Cleave:** That's good for financial systems or electrical utility systems or things that guide transportation systems. All of the things listed on this slide were identified in the President's Executive Order (EO) and in the PCCIP as being critical to the United States (figure 2). I agree with your assurance description.

- **Information and communications**
- **Energy**
- **Banking and finance**
- **Transportation**
- **Water supply**
- **Emergency services**
- **Government services**

**Figure 2**
**Critical Infrastructures**

On the question of what needs to be protected, it's also important to think about what an enormous set of discrete points all those infrastructures represent and what an extensive job it is to protect all of them, and to keep in mind the basics of risk management methodology. I don't know if that's something that you have discussed in this class. If not, let me say that it is the notion that in trying to manage a risk, you don't go out and try to protect and secure all the things that are vulnerable. Instead, you have to set priorities. Setting priorities depends first on identifying what things are most valuable to you; second, what are the vulnerabilities of those things that are most valuable to you; third, what are the threats to exploit those vulnerabilities; and fourth, what are the countermeasures or protective measures that may be

at your disposal to protect these things? Having done an analysis like that, if you are a decision maker, you then have a basis against which you may assign resources to protect things, starting with the highest value, most vulnerable, greatest threat nodes or facilities, whatever they might be, and then scaling it down so that you are maximizing the use of limited resources in management of the risk you face.

**Student:** Do you have another notion or criterion for what is critical infrastructure? What do you mean by critical? What are the criteria for deciding which ones are critical?

**Van Cleave:** The question of what is critical, properly phrased by you, is something that I was subsuming in the issue of what is of value to you. What is critical to you tells you what is really important to you.

**Student:** Not merely to the individual, but to society as a whole.

**Van Cleave:** Yes, at this level. You can apply a risk management methodology as an analytic structure at almost any level. Right now we're talking about what is most critical at the national level, but if you're just talking about protecting your home against intrusions, you could apply it there too. So, it's neutral.

**Student:** I had questions about your slide on critical infrastructures as well (figure 2). Is it according to the priorities that were assigned by the PCCIP? I thought I would take exception to that.

**Van Cleave:** Take a look at them. Do you agree with them? Aren't these the infrastructures that are most critical to the functioning of the United States ... or of most any country, frankly?

**Student:** Not all of those are critical. Some are critical points. For instance, not all government services are critical. Police functions are critical, but some other government services are not. You still need criteria for what you mean by "critical."

**Van Cleave:** I agree. This list is taken out of Executive Order 13010. It is not my list. It's a list that the President signed out as his list. But you're right. Within this list, some things are more important than others. By "government services," I believe that the EO intended to signify continuity of those government services that were essential to the functioning of the nation in time of emergency. "Emergency services" pertains to the state and local levels, like the fire and police departments—those kinds of emergencies. But there are also government services that may be essential to try to recover from an emergency. It's not explained on this slide.

**Student:** I may be wrong, but would the criteria for establishing them in that order then be national security?

**Van Cleave:** National security is a part of what's at issue here, but that's not the whole story, is it? It's also the health of the economy, and the safety of the citizenry. This list is intended to speak to critical infrastructures in time of natural disasters: what the community relies on, what the individual relies on, and what the nation relies on. So it's an ambitious listing in that sense. It tries to speak to all of those concerns in one list.

**Student:** On its ambitiousness, what does it really leave out, apart from entertainment?

**Van Cleave:** They argued about whether entertainment should be in there or not!

**Student:** It's pretty all inclusive.

**Van Cleave:** Yes, I think so, too. Which is an important point, and hold that in mind as we continue.

**Student:** So you mean to say those were in priority order?

**Van Cleave:** No.

**Oettinger:** The interpretation of this at even the individual level is extraordinarily difficult. I'm reminded of the possibly apocryphal stories about the snow emergencies declared in Boston regularly every winter, where every-

body is advised to stay at home unless they have an essential job. Of course, attendance is always alleged to be up on those days because no one feels that they're not essential. So it's a difficult judgment to make.

**Van Cleave:** So, whom or what are we protecting it from (figure 1)?

**Student:** Bad guys?

**Van Cleave:** I would suggest that, with respect to all of these infrastructures, we have regulatory standards (figure 3). All of these infrastructures basically are owned and operated by the private sector in the United States,

- **Either regulatory or market standards for:**
  - Resiliency
  - Failure resistance
- **Vulnerable to disruptions caused by common threats**
  - Natural disasters
  - Normal reliability
  - Nuisance crimes

**Figure 3**

**Nature of U.S. Infrastructures**

not by the U.S. government, but they are publicly regulated. There are market standards and other regulations to ensure the resiliency of these infrastructures to withstand disruptions of various types. Natural disasters, such as hurricanes or earthquakes, that might impact provision of these services pose a well-understood and well-anticipated set of problems. Will they disrupt power or communications? Yes, that happens, so the owners and operators of these systems have contingency plans to deal with that kind of disruption to the system. A backhoe digs up a gas line. They have to be able to handle that kind of problem with their distribution systems. There are also just the kind of normal reliability concerns—equipment wears out, or somebody goofs and throws a switch the wrong way. The owners and operators must also protect against the unreliability of the standard provision of services.

There are also crimes, from low to high levels. People try to find a way to break in and learn what your credit card number is, and what a whole bunch of other people's numbers are, so that they can manipulate the system to accomplish a financial scam of some kind. There are nuisance crimes—vandalism that results in some kind of disruption—up to much larger kinds of crimes, such as bombs or terrorist-type activities.

These sorts of actions, particularly at the everyday level, are the kinds of things the owners and operators of these systems have had to deal with for a long time and continue to have to deal with, and they are a threat, but in today's world, that's not all. In today's world we have a new kind of threat to these infrastructures that has become a concern, and that is the cyber threat.

Some 100 foreign nations may have the capability to pose some kind of threat to U.S. infrastructures, which in large part is a function of the fact that the tools for hacking and the techniques for accomplishing harm, and the information needed to plan a course of attack, are pervasive and readily available (figure 4). There are some 25+ countries where there are terrorist groups and other

- **Nation-state sponsored**
  - Over 100 foreign nations with capability
  - Some with "infowar" efforts
- **Independent actors**
  - 25+ countries with computer attack groups/mercenaries
  - Most are very sophisticated/competent
- **Tracking the origin of any attack will be very difficult!**
- **A defensive IW warning system will be a critical part of our future construct.**

***The threat is multidimensional, multifaceted, and growing!***

**Figure 4**

**Where's the Threat?**

kinds of groups that may have some of these capabilities; that is also kind of a rough number. But, again, it's a result of the fact that these kinds of tools, unlike other sorts of weapons, are so pervasive and so dual use and so readily available that they're spreading.

For planners in the United States, or anywhere, who are trying to protect against these kinds of threats, discerning where the attack originated is a very difficult endeavor, especially recalling our opening discussion about the permeability of borders and that sometimes you can't know whether you're dealing with a domestic or a foreign event. The last point on this slide is that having a warning system against an information attack is a pressing need, but also a very difficult one to fulfill. It's something that I will come back to and discuss in a little more detail in a minute.

**Student:** I don't know if you compared countries that sponsor classical terrorism and those 25 countries that have cyber terrorism. How many of them overlap? In other words, among those 25 countries, how many of them are U.S. allies?

**Van Cleave:** Some are, but this is sanitized information from classified sources. So I can't give you any more detail except to say that some are traditional allies and some are the usual suspects—you can be pretty confident of that.

So, from the national security point of view, we have reached a time in our nation's history where society depends on various interdependent systems and so does the military (figure 5). We were discussing earlier the military reliance on commercial satellites and communication systems, and the opportunity they provide to do things more flexibly and perhaps with some redundancy and backup. At the same time, that creates vulnerabilities that one has to be concerned about in designing our communications architecture.

Today, the military depends to an enormous extent on commercial infrastructures, because that's the most efficient way of doing business. It used to be that the military and the intelligence community were on the leading edge of much that we did technologically,

- **Modern society depends on complex, interdependent systems, interlinked through communications networks, to achieve maximum business benefit.**
- **For the military, it is no longer cost effective to have separate communications systems.**
  - Interconnectivity is needed for the conduct of modern military operations.
  - Utilization of commercial products, communications infrastructures, and complex software is essential.
  - Interoperability with joint and mulitnational coalitions mandates use of broadly accepted commercial standards.

***Cost considerations will continue to increase dependence.***

**Figure 5**

**Network Dependence**

but today the commercial world has caught up in many, many ways and even surpassed what we're able to do through the military and intelligence pieces of the government. This is particularly true in information technology. This interdependence is only going to increase as time goes on. The other point is that because the United States has the most highly developed information technology, and is the most network-dependent nation in the world, we're also the most vulnerable to information attacks that would exploit these networks for gain (figure 6).

It may be worth taking a moment to think about what we mean by an attack on infrastructure. In warfare, infrastructure targets have long been part of traditional targeting strategy. If you look at what's going on in Kosovo, it is true there. We're looking to attack and destroy with a bombing campaign key facilities that are important to Yugoslavia's industrial support to its military capability—a traditional type of target. So there's really nothing new in that. What is new is the networked nature of these infrastructures today and their dependence on computer technology, and the opportunity that could present to an adversary who is prepared to take advantage of it. What we're contemplating now is not just discrete physical destruction

- **Massive networking makes the U.S. the world's most vulnerable target for IW.**
  - Intelligence exploitation
  - Disruption of network infrastructure
- **U.S. has orders of magnitude more to lose to IW attacks than its competitors.**
- **Reliance on *unprotected networks* carries *risk of military failure* and *catastrophic economic loss.***

***We are the most vulnerable nation in the world!***

**Figure 6**

**How Vulnerable Are We?**

and the need to be vigilant against that, but the possibility that an attacker could disrupt, or interfere with, or even in some sense shut down much larger parts of the U.S. infrastructure through a cyber attack.

I don't want to suggest that infrastructure protection is somehow a new concern of the United States. Being able to protect key facilities against physical destruction has always been a concern, but what has brought this issue to the forefront is really the cyberwar threat to infrastructures that are so interconnected because of the networked nature in which they run. I'm making an assumption here that, having read the PCCIP report, you all know that all of these infrastructures are maintained and operated and driven by computer controls and are wholly dependent upon them. They are in many ways interdependent, so that an attack on one part of one infrastructure may have cascading effects into other parts of the infrastructure and the damage could extend much further than a single or discrete attack. For example, if a dam is taken out because of explosives planted by a terrorist group, that's a horrible thing. But if the electric grid is penetrated by a group manipulating cyber access, that could potentially take out a much larger part of the electric power grid. At least that's a concern.

When people think about IW concerns today, they think about hackers, even hackers who may be home bred and are testing their skills in intrusion against different targets to see how far they can get. We see this kind of thing every day, of course. If you talk to representatives of the telephone companies, they will tell you that all the switching centers in the United States are constantly under attack by people sitting at home playing with their computers, using the Internet as a toy, and trying to break in and see what they can do. Some of them are social miscreants looking to do bad things, and vandals, so there's a little bit of that in there. There is also criminal or terrorist interest in some of these things. All of those are a concern, but the added concern is the potential ability of a foreign nation to develop a capability to hold U.S. infrastructures at risk, in a strategic sense, in a way that could potentially coerce the U.S. government to do or not do something else (figure 7).

Have you done any reading at all in this area of IW capabilities?

**Oettinger:** Greg Rattray has spoken to the class. One of the earlier readings was his thesis on strategic IW.[1]

**Van Cleave:** Great. I participated in designing and running a series of war games in 1996 for the RAND Corporation, at the direction of the Office of the Secretary of Defense. We were designing these games to test how decision makers would deal with a situation in which there was a strategic attack, or there was a disruption of some essential U.S. systems, and how that might affect their decision making in the course of a conflict. We ran these games starting at a working level and going up through the sub-cabinet level. John White was deputy secretary of defense and sat in on the last game that I moderated, along with General Ralston, vice chairman of the Joint Chiefs, and General Minihan, who at that point was head of NSA. He has recently left.

Of course, it was very interesting to see how the domestic backdrop, the public reaction to essential services being denied—blackouts or disruptions, interference with

[1] See Major Rattray's presentation in this volume. The title of his thesis is "Strategic Information Warfare: Challenges for the United States" (Tufts University, 1998).

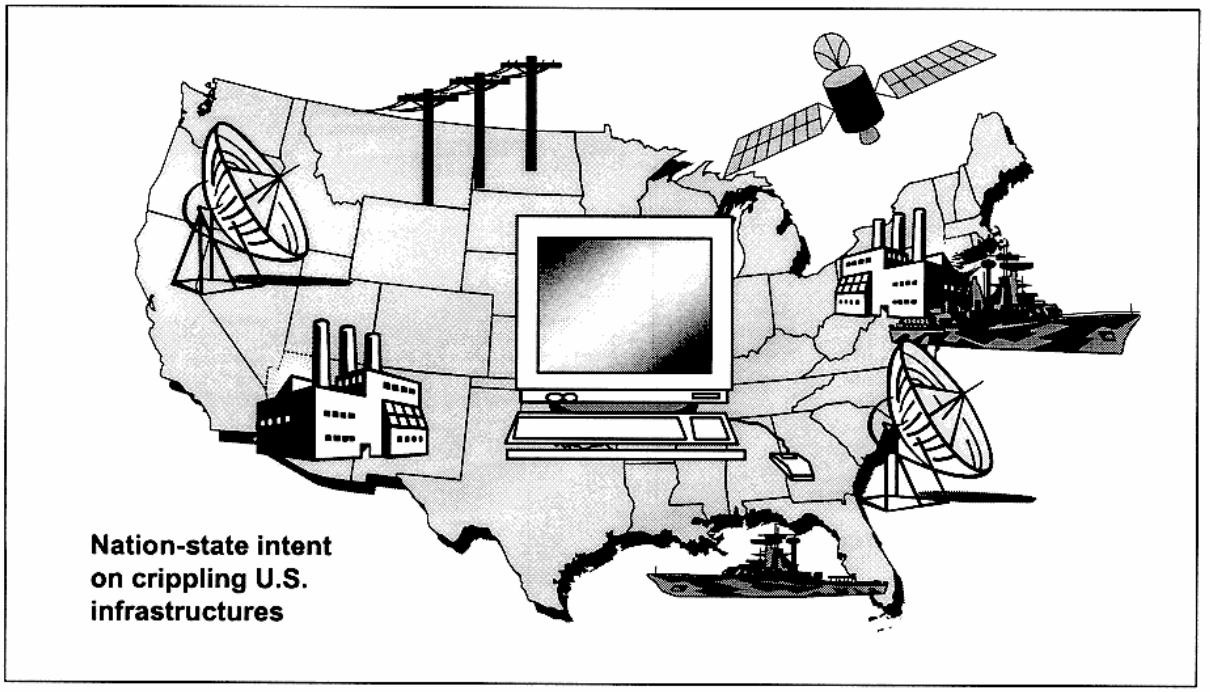



**Figure 7**
**Likely Threat in 5–10 Years**

the financial market spreading loss of confidence, or telecommunications outages so that people couldn't talk to one another and didn't know what was going on—would affect decision makers and their willingness to do or not do certain things in the course of a conflict. For those of you who have not participated in them, I would say that war games like that are very interesting learning tools for trying to test out different approaches on policy. There's nothing like getting a group of people together, putting them in a situation, building the scenario, and asking them to role-play, particularly if they're bringing their day-to-day jobs and responsibilities to the table anyway, to elicit understanding of some of the real issues. When they're well designed, I found these games to be very good tools in developing policy, at least at the level at which I have engaged in them before.

As it happens, we did some role-playing in these RAND games that gave some insight into the potential impact of these kinds of events. But there were also larger-level exercises and one real-world event that I want to mention to you that you may or may not know about. Do you know about the Eligible Receiver exercise? Eligible Receiver is an exercise run by the Joint Chiefs of Staff every year, and every year it has a different focus. In 1997, Eligible Receiver played out another scenario where a big part of the game was dedicated to IW, or attacks, or disruptions in the U.S. infrastructure in the course of an effort (in this scenario) to deploy forces abroad. Eligible Receiver is an exercise, which means that the actual units that would be involved in the deployment were deployed, and at sea, or called in to be ready to go. All the logistics train, everything that goes along with it, was brought into this exercise that took all year to prepare. People were really in the field over a two-week period.

The exercise also included a Red Team, a cell at NSA, that used open sources to develop attack capabilities against key U.S. defense computer networks, military networks, which they in fact carried out in real time against those networks to see how far they could get. They also had profiled attacks against infrastructure—civilian networks—that they didn't carry out, but they simulated what those would look like. The upshot of Eligible Receiver '97 was that deployment in the Pacific was halted because of the confu-

sion and disarray and uncertainty that they were able to introduce into the command and control of that deployment. The exercise stopped early because the Red Team was so effective early on. It was a very sobering experience for everybody involved regarding the potential of using IW disruption in the course of a military engagement.

Soon after Eligible Receiver '97, there was a real-world event that received the name Solar Sunrise. Solar Sunrise was a series of intrusions into defense computers that occurred early last year, at a time when the United States was in a period of great tension with Saddam Hussein, and it looked as though it might be necessary to redeploy to the Gulf. As it happened, we didn't, but it was learned that these intrusions were originating from outside the United States, somewhere in the Middle East. It was a very alarming set of intrusions because of the particular systems that were attacked. It resulted in the President of the United States being briefed that it wasn't clear to us, but that it was possible the United States could be under an IW attack emanating from Iraq.

Later (I'm talking now about a week and a half to two weeks into this series of intrusions) it was learned that this was not Iraq. In fact, the origin of this attack was in Israel. It was being routed through other countries in the Middle East before it came back into the United States, but it was orchestrated by an individual in Israel who was also using young people in the United States who were participating in this attack. But it took quite a while to figure that out. We didn't know for some time who was responsible and why—another learning experience.

**Student:** I've also heard that how they found out inadvertently was someone making a call at random and asking if similar system failures had occurred in their organization. I was just curious if the lesson learned from that exercise was a greater need for communication across units, across services. I think it was the Air Force who got credit for this, but someone just had some unusual occurrence and thought to call someone else, even though he knew they weren't related, to test his own intuition on that.

**Van Cleave:** There were a lot of individual contacts—people picking up the phone and asking, "What do you think about this?" The way that the attack profile was finally broken was all very informal. It included the fact that there was an NSA representative sitting over at the FBI who persuaded the Bureau to bring some of what they had over to NSA for traffic analysis. You would think that would be common procedure, but it wasn't. It had to be done in an ad hoc fashion. That type of piecing together bits and pieces still characterizes the way we're dealing with these kinds of intrusions.

**Student:** On this attack that you called Solar Sunrise, did they have any information on motivation? Was it just somebody showing off, or what?

**Van Cleave:** Just somebody showing off, right. This guy has now been drafted into the Israeli army. He wasn't before; he is now.

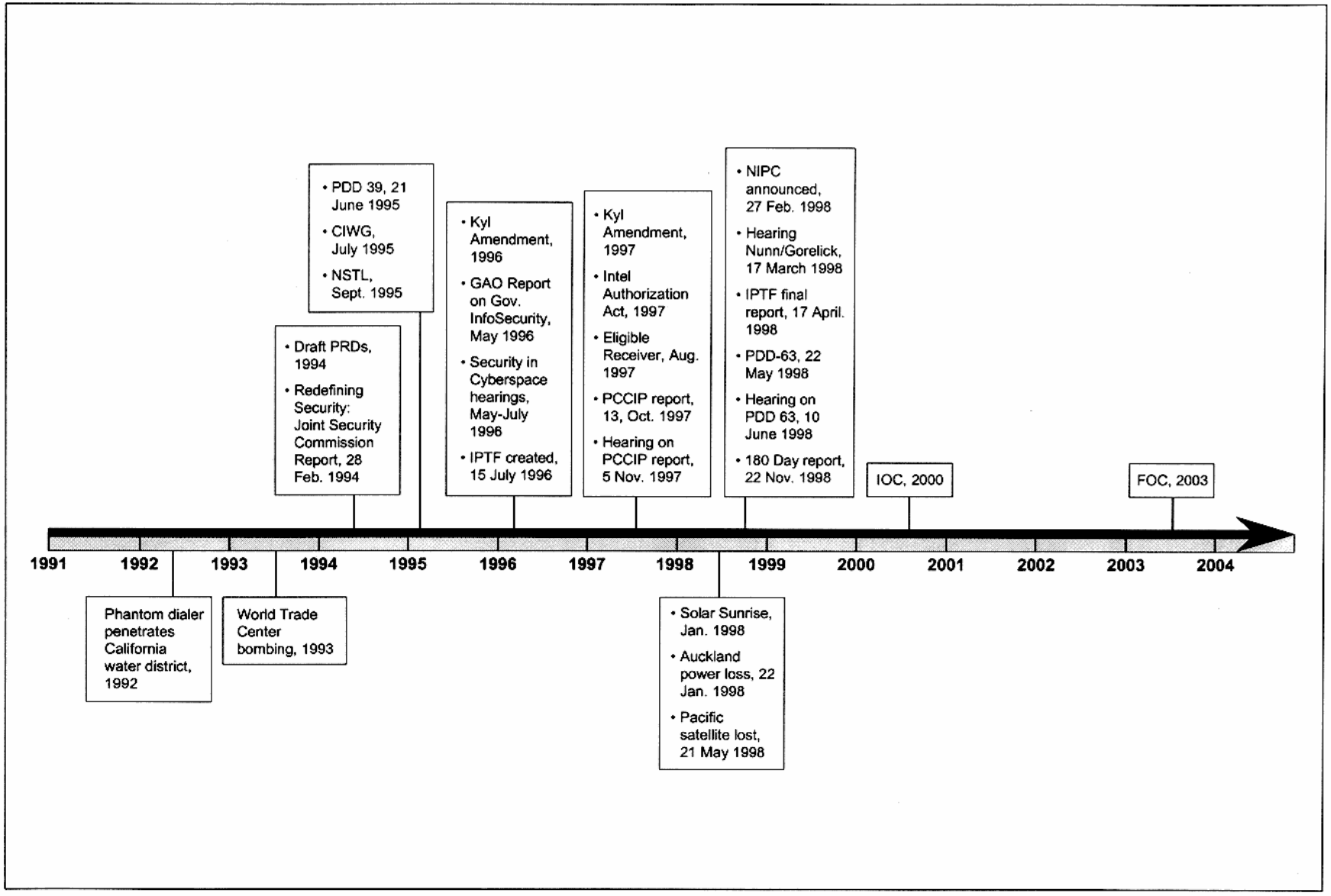
The notion that we need a policy to protect the nation's critical infrastructures has some antecedents to it. I think it might be useful just to take a moment to talk about what they are. This little timeline actually includes other things as well, but it leaves some things off (figure 8). After all, time didn't start in 1992.

Let me just remind you of some of the policy antecedents that will bring us up to where we are today before we launch into that. What's not on this chart, and what is worth noting, is that in 1981 President Reagan signed Executive Order 12333, which you all should be familiar with, having to do with the oversight and the conduct of intelligence activities. It established the procedures by which intelligence could be shared with law enforcement, so 12333 is important to us in that regard.

**Oettinger:** I might just interject for the record that Phil Heymann's 1997 presentation goes into some detail on that EO, so those of you who would like to pursue that further can read up on it.[2]

---

[2] See Philip B. Heymann, "Relationships Between Law Enforcement and Intelligence in the Post-Cold War Era," in seminar proceedings, Spring 1997.




CIWG = Critical Infrastructure Working Group
NSTL = National Security Threat List

**Figure 8**

**Critical Infrastructure Protection Timeline**

**Van Cleave:** Another EO not mentioned here, but also germane in the infrastructure protection arena, is Executive Order 12656, which was signed in 1986, also by President Reagan, assigning responsibilities for national security and emergency preparedness (NS/EP). Now, what is NS/EP? It is a term applied to the contingency plans that the government has working with state, local, and private industry to deal with all kinds of emergencies that may impact the nation's security from natural disaster, such as hurricane recovery, to surviving a nuclear strike. These plans ensure that critical services and infrastructure are maintained, including the flow of critical information.

Let me talk for a moment about what we mean by infrastructure assurance and what we're assuring it to do (figure 9). NS/EP is in the middle. Let me describe what I see as three different baskets of activities that are involved in infrastructure assurance.

Industry, as we've already discussed, has responsibility for ensuring the reliability and robustness of the services that it provides to all of us as customers—individual, corporate, state, or federal government—of these services. They must provide for the security, safety, and reliability of their operations. For business planning, this includes contingency plans, so that if there is a flood and your factory is rendered inoperable, insurance (and sometimes industry standards and sometimes regulation) requires that you have backup, redundant capabilities, so that you're able to continue to provide services when there are these kinds of disruptions. So business contingency planning includes a lot of different things, but they're part of the usual kind of work that is done by the infrastructure owners and operators.

In the area of NS/EP, in Executive Order 12656 the federal government plans for how to deal with emergencies when they arise. A part of federal government's planning, in concert with state and local government, is to ensure that essential services—some of these infrastructure services—needed for dealing with emergencies will be available. Again, this runs the gamut of possibilities. If you've got a natural disaster, what are the government services that you must have up and running to deal with the consequences? Or if you have a war, what kinds of things must you be able to do in the course of dealing with the effects of that war on the civilian population? These things are part of NS/EP planning: traditional kinds of planning that are not limited to infrastructure services continuity, but do set requirements for infrastructure services that are necessary to provide these emergency services by the government.

What does that mean in practice? In practice, that has meant such things, in particular, as the creation of the National Communications System (NCS), the agency within the government made up of 26 departments and agencies that have telecommunications responsibilities for the federal government. It was created by President Kennedy in the aftermath of the Cuban Missile Crisis because the telecommunications overload that occurred at the time really impaired some of the essential communications the government needed to deal with that crisis. Kennedy recognized that we must have some way of prioritizing access to limited communications. So he created the NCS, which originally

| | | |
|---|---|---|
| • Convenience and commerce services | • Minimum essential government services | • National strategic capabilities |
| • Security, safety and reliability | • Reliability, redundancy, priority reconstruction | • Indications and warning |
| • Business contingency planning | • NS/EP disaster planning | • National defense planning |

**Figure 9**

**Roles and Responsibilities**

operated through AT&T (the only telecommunications carrier in the nation at the time), to work with the telecommunications infrastructure, to make sure that these emergency capabilities were always available.

When Judge Green broke up AT&T, part of his order to the regional Bell companies was that they would continue to work with the government to ensure that there were emergency services. President Reagan set up the National Security Telecommunications Advisory Council (NSTAC), which brought together the various telecommunications carriers so that they would be able to advise the federal government on emergency requirements and the state of the telecommunications network. Those of you who follow telecommunications reform will be aware that the market has now been opened up, regulations have been removed, and there are a lot of new players providing telecommunications services. This raised questions for those in the government who are responsible for NS/EP and planning of continuity of communications in times of crises. It's much more difficult to deal with the open market than it is to deal with the monolithic AT&T, or even a handful of regional Bell companies, as was the case in the 1980s.

**Oettinger:** Again, if I might just interject here as a reminder, you've heard General Kelley, the current director of the Defense Information Systems Agency (DISA). His predecessors in that agency, and its antecedent, the Defense Communications Agency, are represented way back in the beginnings of this seminar.[3] So, if you want to track the history of this particular development of the NCS and the NSTAC and so on, you will find that in the record. I think it's valuable to do that because if you want to know about current problems, and how quickly they get solved or how they get addressed, this set of problems did not come out of the blue. It has a long history, and it's instructive to understand that history.

**Van Cleave:** For example, General Kelley is the manager of the NCS, in addition to being the head of DISA. In the middle column, for emergency services planning, DISA has a program for telecommunications priority restoral, so that if things go out, you have priority users identified, and the phone companies know they have to work to get these particular circuits up first. That kind of advanced planning is what the telecommunications industry has been doing for years in working with the government to try to ensure communications continuity.

There are also emergency contingency plans in other areas. They are less well developed than in the telecommunications arena, but they nonetheless exist. FEMA, the Federal Emergency Management Agency, is the outfit responsible at the federal level for marshaling and coordinating all of these various resources. So, what happens here is that you have a priority user, the federal government, defining its requirements, disseminating them to the infrastructures, and having the infrastructures come back with contingency plans. It is driven from the top down.

In the business category of infrastructure assurance, you have the owners and operators, responsible for all of the customers, trying to anticipate what the disruptions could be and to ensure equal continuity of services in all areas, as much as possible, in a reliable and safe way. It's not driven from the top in that sense. The robustness of the network as a whole is really at issue here. So there's a different kind of analysis or analytic planning for infrastructure assurance or infrastructure protection; two different approaches for two different purposes. They obviously fit together and have relationships between them, but analytically they're different.

The last column is what's new in the arena of strategic IW. What we are concerned about in this category is the possibility that a foreign adversary could look at the infrastructures of the United States as a target with strategic value, and seek to target critical nodes within the United States for disruption

[3] See General Kelley's presentation in this volume. See also Albert J. Edmonds, "Information Systems Support to DOD and Beyond," in seminar proceedings, 1996, and "Integrated Information Systems for the Warrior," in seminar proceedings, 1995; John T. Myers, "Future Directions for Defense Communications," in seminar proceedings, 1989; and Lee Paschall, "C$^3$I and the National Military Command System," in seminar proceedings, 1980.

or destruction. That is a national security strategy analysis, which says, "This is a threat, it is a strategic threat, and we need to have a strategy to counter that threat." It may have several elements, which we will get into. It is strategic thinking, looking at how we ensure essential services should there be a terrorist disruption or a natural disaster or even war, to make sure that we have and continue to function as a government.

All of these things are part of infrastructure assurance. Each has discrete roles, responsibilities, missions, and purposes. They complement one another. But the reason why I've taken some time to go over these different approaches with you is so you have in mind that when people talk about infrastructure assurance, they may mean very different things, depending on the perspective from which they're looking at protecting our infrastructure. Is it protecting against the hacker who might come in and disrupt services so that your phone goes out because someone has messed around with that system and it needs to be fixed? Is it someone who is responsible for these contingency plans, who looks at the infrastructure support and what kinds of emergency or backup or redundancy programs he has to put in place, most likely because of collateral damage of some kind to the infrastructure—collateral to a natural disaster, or collateral to an attack? That's an infrastructure protection problem, too.

Lastly, there's the new one—strategic IW, and the strategy to protect the infrastructure. Is there a strategy, for instance, to deter an attack against the infrastructure? What should the declaratory policy be? The strategic questions here are not yet answered.

**Student:** I was wondering if you could talk a little bit about the conflicting relationship, in that it seems that a natural response to the latter two issues would be to sort of assign some downstream liability in the event of an occurrence. Then you'd have the businesses that originally were looking toward universal access, including redundancy, facing the threat of this liability. For example, if an electrical power company were held responsible for all the damage that happened as a result of the power going off and had to replace everyone's food in the refrigerator, that would be huge impetus to degrade the convenience and commerce services. At the heart of it is this sort of infrastructure protection concept.

**Van Cleave:** Some of the liability questions are really contentious. In the middle category, in the area of traditional planning for continuity of services by direction of the government, liability is removed from those companies that are participating in a certain way, pursuant to government order. The infrastructure owners and operators would much prefer that if they're going to do something, it's because they were ordered to do it, and they don't have any liability exposure as a result of it.

In the first category, there are lots of private contracts now between service providers and their customers that allocate responsibility or limit liability in the event there is a service outage. I'm not familiar with this area of the law (maybe there are others here who are), but if you are a plant that offers refrigeration services for frozen goods and you need to have electric power in order to continue to keep your inventory current, you may want to include in your contract with the power company providing your services that they are liable to the extent that you lose your goods if the power goes out. So there is opportunity to allocate responsibility that way with a private contract.

**Oettinger:** I'm thinking that's the tip of a huge iceberg of great contention, because it isn't only the liability issues, it's also competitive issues over what you do as part of normal business and how you shave costs. You've got every businessman having a balancing act there, and the balances struck for competitive purposes may have no relationship to the balances struck for the other two purposes, so the norm on the left-most column here may be at total variance with what might be desirable for the other two. I'm so glad that Michelle gave us that diagram, because it points up why this is such a messy and difficult area to deal with. This metaphor of reconciling the three columns is a particularly powerful one, for which I'm grateful.

**Van Cleave:** To pick up on the liability issue, a business that provides information about intrusions into its vital networks or its own vulnerabilities may be exposing itself to liability or shareholder actions if the government entity to which it provides this information (because the government is trying to figure out what to do about it) handles that information in a careless way and it becomes public. It can have commercial repercussions and liability repercussions on that company if, for instance, part of the information that it's giving out has to do with one of its service providers. This has been a problem in gathering information about what the real vulnerabilities are in the first place. It's also a problem, in figuring out how you're going to put together a national strategy or architecture to try to protect the infrastructures, to know how information can be passed and received and handled so that there isn't exposure or liability.

This brings to mind that in my work on the Judiciary Committee, one of the last things we did was to pass a bill having to do with liability on Year 2000 matters. One of the problems in Y2K remediation has been that talking about remediation efforts could cause some people to rely on that information that you, the manufacturer, have provided. If it turns out you were wrong and your remediation hasn't worked, and the customers have relied to their detriment on your representation that you've taken care of this, then the concern was that they're going to sue you because of that. So the Year 2000 Disclosure Act held companies that provided information about their remediation efforts harmless from any additional liability arising from those statements. They could still be held liable for any harm that was caused by their failure to remediate, but you couldn't sue them and say, "Hey, but you told me this was going to work!" That is not an additional cause against them.

The liability matters in the infrastructure arena, and many major Y2K concerns, are infrastructure reliability concerns. There's a lot more to it, obviously, than that. But at the national planning level, I think, we're most concerned about the robustness of our infrastructures in light of Y2K difficulties. So the liability problems were the first things that industry came to Congress about. There are more bills pending now. That was a very, very small step, but these liability questions are big. So it might be right to work them out.

**Oettinger:** Now that we're a bit further along in this semester, if you put Michelle's comments in the context of Kawika Daguio's remarks,[4] specifically about the financial services industry, I think if you go back to your notes on that, you'll see them in a different light now that you've heard today's presentation.

**Student:** Do you feel that nonattributional reporting in that sense has set a precedent, and it's going to happen more and more as some other architecture protection issues arise after 2000?

**Van Cleave:** Yes. Generally, my message on Year 2000 is: I've all kinds of concerns about it, but if there's anything good that will come out of it, it is increasing awareness about the need to have robust architectures in your infrastructure and making sure that you have redundancy and other reconstitution capabilities in place. So there is a silver lining to that Y2K cloud, but that's still somewhere down the road.

The other silver lining to that Y2K cloud is that we're not going to be able to anticipate or to know what kinds of disruptions will occur because of Y2K, but we can plan. The private sector is doing this work. All the planning, all the work, whatever it is that everybody together does, will have whatever effect it has, and there will be things that will need to be fixed. That may take some time, and it's hard to know how expensive or how puny those disruptions may be. But one of the things that we need to do as a government, as government planners in the area of infrastructure protection and national security, is to have good diagnostics to observe the effects of Y2K disruptions, because they're likely to resemble what a handful of IW attacks might look like on particular networks. If we can learn from the way in which those kinds of disruptions are handled,

[4] See Mr. Daguio's presentation in this volume.

and from the organizational thinking and the processes that are necessary to go into handling those things, we will be ahead in understanding wise planning for infrastructure disruptions that may be deliberate and not Y2K induced.

So I think there is an opportunity to learn from the experience that we're going to have. It's kind of gruesome, but you're faced with it.

**Oettinger:** One of the things that sort of concerns me, and I don't know whether this is fantasy or real, is the question of introducing more errors in the process of fixing things. My impression is that the world is now full of contractor Y2K fixers of varying abilities, and given the history of writing software, the odds are that in the process of fixing the Y2K bug, they're bringing in new ones. Am I being paranoid?

**Van Cleave:** Not at all. The concern is that inadvertent mistakes will be made, and then there are purposeful things that may be done in the course of this. There is such a frantic pace of effort, and so much going on right now, that quality control always suffers under those circumstances. I participated in the work leading up to setting up the Year 2000 committee in the Senate, which Senator Robert Bennett [R-UT] chairs, so I've been involved in a lot of the reports that have come into that committee and heard a lot of the anecdotal information that has come in as well. One that I recall is a story about a particular facility that had brought in a team to do its Y2K remediation, and when that was complete, went back to do its own private check with a separate team to see whether other changes had been made in the course of the Y2K remediation. This was a financial institution, and, in fact, a whole series of backdoor entries had been built into the system that hadn't been there before. You could say, "Well, that could be benign. It could be that those who had done the remediation were looking for quick ways back in case problems developed and they wanted to be able to have quick access." Or you could have a different interpretation.

But the opportunity for things being done in the course of this is very real. It's also true that many software fixes are being done offshore, and questions arise. There is no really good way of getting a handle on that because the time urgency is so real, and people are taking shortcuts and maybe not taking the kinds of precautions they might otherwise take.

So, could we be setting ourselves up? If you are a foreign adversary who takes the possibilities of these IW tools seriously and is looking somewhere down the road, some of this has a very long lead time. One of the things you need to be able to do is to build in the access you need in order to accomplish some things. Taking advantage of the Y2K phenomenon is sort of an obvious thing that you would expect a determined and thoughtful and patient adversary to do. So, yes, there are issues being raised by this. At the same time, there are improvements going on. People are taking a look at the reliability and security of information systems in a way that perhaps they haven't before, and there are opportunities to upgrade. So, there is a little good and a little bad.

**Student:** You can make the same argument about giving $10 billion to a company to fix your own governmental computer systems. Since in the United States you have to hire U.S. companies, you will think twice about letting those people into your systems.

**Van Cleave:** Yes. Now, back to the timeline (figure 8). This again shows some of the things that have gone on as predecessors to where we are now. If you haven't seen the Joint Security Commission report, which was issued in February 1994 and chaired by Jeff Smith, the former CIA general counsel, it's an excellent report on government security that addresses all different parts of security, including information systems security. That commission made a lot of recommendations on how to improve things that were not implemented.

Also back in 1994, the Department of Defense, largely at the instigation of the late General Frank B.W. "Barry" Horton, looked at trying to direct a study on offensive and defensive IW strategy. Those drafts floated around for a while, but ultimately died, largely because of John Deutch's opposition

to putting out a Presidential Review Directive, which is what PRD stands for, for interagency coordination. Sometimes it's interesting to see that if you need to have policy developed, some people may be unwilling to have the President issue a directive involving all departments and agencies, because then nobody controls what comes out at the end. You lose control of the process, and by the reports that I've heard, that was really John Deutch's concern. He didn't see how he could gain and keep control of this if it went interagency, and so the PRD effort died.

In June 1995 Presidential Decision Directive (PDD) 39 was issued, the PDD on counterterrorism. Among other things, that PDD assigned responsibility to the attorney general to constitute a team to look at cyber terrorism and what to do about it. She was given that lead responsibility, and pursuant to that responsibility, she set up the interagency Critical Infrastructure Working Group.

The National Security Threat List, issued in 1995, is the list of things that the FBI looks at when assigning counterintelligence resources: the things that need to be protected from foreign intelligence threats. In 1995, critical infrastructure nodes or facilities were added to that list as a counterintelligence concern of the FBI.

In 1996 my former boss, Senator Jon Kyl, added an amendment to the Defense Authorization Act that directed the President to submit a report to Congress on the elements of an architecture for indications and warning (I&W) of a strategic attack on U.S. infrastructures. It also directed that the President report to Congress on the future of the NCS, which we were talking about a moment ago, and how the assets and experience of that agency might be brought to bear in the IW arena. That report has never been submitted.

There was a General Accounting Office report on information security that talked about some of the problems with the government. Senator Sam Nunn [D-GA] held hearings on cyber threats to government information systems. The records are also good resources for those doing research in this area.

Executive Order 13010 was written by the President in July 1996, and in a letter back to Senator Kyl, he said, "I am setting up a new commission on critical infrastructure protection that will study the issues that you have raised, and then we'll get back to you on the Kyl amendment of 1996." Simultaneously, the Infrastructure Protection Task Force (IPTF) was created at the FBI, with interim responsibilities for infrastructure intrusions.

Senator Kyl had another amendment in 1997, which said, "We understand that you're working on this, but you also need to give us a report on what a national strategy to protect the infrastructures would look like. In addition to indications and warning, what is the large strategic context in which all of this would arise?" The Intelligence Authorization Act directed the DCI, the director of central intelligence, to report on the intelligence component of the strategy to protect against IW threats, also a Kyl initiative.

Eligible Receiver we've discussed: that JCS exercise. Then the President's Commission report came out, which we're going to go into only very briefly because General Marsh will be describing that to you in more detail. The Solar Sunrise incidents occurred. Maybe you remember that in Auckland, New Zealand, there was a time when they lost power practically through their entire city for months. It was quite a serious disruption down there. The National Infrastructure Protection Center (NIPC) is an entity of the FBI that grew out of the IPTF. I'm going to go through all this when we get into the PCCIP.

**Student:** Could you please discuss the difference between an Executive Order and a Presidential Decision Directive? I think I've got the essence of it, but I want to be sure.

**Van Cleave:** Executive Orders are executive decisions that tend to have more permanence than a Presidential Decision Directive or a National Security Directive (NSD). EOs stay in force unless they are specifically revoked. PDDs and NSDs are issued by the President. EOs can pertain to anything; PDDs and NSDs are all national security directives by the President. (Tony, you leap in here.) In practice they have equal dignity as far as the agencies and departments of the executive branch are concerned, but the PDDs and the NSDs tend to be the kind of thing that a new

administration will review and might change more readily than the EOs.

**Oettinger:** It's exactly that pragmatic distinction you make, because the formal distinction has never been clear. In several administrations that I've watched, they don't touch the EOs, but the first thing they do when they come into office is look at the previous PDDs and NSDs and change the nomenclature, because somehow it seems a macho thing to call it something else so that you get totally confused.

**Student:** That's true everywhere.

**Van Cleave:** Do you know what I've observed? Democrats always call it a presidential blah, blah, blah, and Republicans always call it a national one.

**Oettinger:** They play weird little games like that, and they spend the first six months rewriting or canceling the previous administration's orders, and then life goes on. I have no idea what goes through people's heads when they say "We're drafting an EO," versus "We're drafting one of these PDDs or NSDs."

**Student:** It sounds to me as though a PDD is more of a policy letter. Take the military aspect. A commander would say, "Okay, as long as I'm boss, this is to be enforced. This is my directive as the commander. After I leave, of course, if somebody wants to change it, fine and dandy." But the way I understand it is that an EO is a law. Is that correct?

**Van Cleave:** It's not a law in the Constitutional sense, where the only laws are those that are enacted by the Congress and signed by the President. In that sense, it's not binding on citizens.

**Oettinger:** No, but they are instructions to government agencies in carrying out the law arising from the President's responsibility under the Constitution. They say, "Under the authority granted to me by Public Law such-and-such, or something like that, I direct the Department of Commerce to do this, or the DCI to do that."

**Van Cleave:** They're all public documents.

**Oettinger:** The EOs are.

**Van Cleave:** But the PDDs are not.

**Student:** Correct.

**Van Cleave:** Even the Congress is not entitled to see PDDs.

**Student:** I knew that.

**Student:** What's the logic in that?

**Van Cleave:** Because it's all within the prerogative of the President to carry out his responsibilities as he chooses.

**Oettinger:** It's privileged.

**Van Cleave:** It's just the same reason why members of the National Security Council (NSC) don't testify before Congress.
**Student:** They are typically the folks who actually write the PDDs.

**Van Cleave:** Exactly. They're the President's staff.

**Oettinger:** Maybe the EOs are public orders and the other things are sort of internal executive branch ruminations.

**Van Cleave:** Another distinction is that EOs can be about anything, and PDDs and NSDs are all national security.

**Student:** Where do they sit vis à vis federal regulations?

**Van Cleave:** Federal regulations are the federal agencies' interpretations of how they're going to carry out the laws that have been enacted by the Congress. The federal regulations must be published for public comment before they can be implemented. So it is how the laws, once they're enacted, are in fact implemented by the departments.

**Student:** Would regulations enjoy a higher effect? They're almost in between EOs and statutory enactments.

**Van Cleave:** Yes, although EOs do not speak to the responsibility of citizens, and they do not create any obligation on the citizens. What they do is direct the departments and agencies on how to act. Federal regulations are regulating you, the guy up there who has the business or whatever it is.

**Oettinger:** NSDs and PDDs are internal documents. They are inside memos, essentially, as opposed to communications with the real world.

**Van Cleave:** Right. As an example, let's take Executive Order 12656, which assigns responsibilities for national security and emergency preparedness. It says, "It shall be the policy of the United States government to ensure that essential services can be provided across all kinds of ...," versus a policy statement, where the introduction is what the policy is. Then it will say, "The purpose of this Executive Order is to assign responsibilities to departments and agencies to ensure that these policies are carried out." The third part will be, "The secretary of defense is directed to ..." and it lists all that stuff. "The secretary of the treasury is directed to ... , and the DCI shall do *this*," and "There shall be created an interagency group that will review *this* and do all *this* at a policy level." It's the President organizing himself through an EO that sets all of this out.

You can have some PDDs that are very similar to that. For example, the PDD on counterterrorism, number 39, basically concerns itself with roles and missions: assigning who is supposed to do what. Sometimes they can look a lot alike.

**Student:** I was going to say that PDD 56 sounds like the one you just mentioned previously, the one that talks about the interagency process and all that stuff.

**Oettinger:** PDD 63 is rife with interagency direction; it creates a couple of entities, and directs coordination.

**Van Cleave:** I'll tell you in a minute why I think 63 is a really poor PDD. It's very poorly written and poorly conceived. It's not a good example of how you should go about doing this if you're running the show.

**Student:** Are any of those ever classified?

**Van Cleave:** No, but PDDs can be.

**Student:** I have a question on the PDDs, and maybe it's different with EOs. They have no real teeth. If the President puts out a PDD and it's not followed to the letter, who is accountable for that?

**Van Cleave:** That is one of the essential responsibilities of the President's staff within the Executive Office of the President. The NSC staff has two major areas of responsibility. One is to coordinate department and agency activities, and to act as a facilitator, and as part of the coordination to develop policy and options for the President's consideration. The other is that once the President has said, "This is the way it's going to go," then it is the responsibility of the NSC to make sure that the President's directions in the national security arena are being implemented. So they're the watchdogs of the departments and agencies to make sure that they're carrying out the President's intent.

**Oettinger:** That doesn't mean that things happen seamlessly. I have a vivid recollection of a very senior, now retired, military commander throwing me out of his boss's office where I was on a mission of exactly the type that Michelle describes on behalf of the NSC. He said, "We are not in the habit in letting you intelligence weenies mess around with operational matters." So I took my tail and put it between my legs and went back home and reported it to the boss. I don't know what happened next. The responsibility is there, but that doesn't mean the last word. There's a lot that goes on between the signing of an order and its execution. That's as true of the commander in chief as it is at a battalion or squad level.

**Student:** When I was on the Joint Staff, we used PDDs a lot as our source documents

for, justification for, or backup for regulations within DOD. In fact, we created a new DOD directive based on one of the PDDs on senior leadership travel. We went back and used that as a source document and said, "This PDD says *this*, therefore we're going to create this DOD directive to say *that*," and then everybody said, "Fine."

**Oettinger:** We only have about 10 minutes or so left if we're going to get you on your airplane. And so, your comments on that PDD 63 would be warmly welcomed.

**Van Cleave:** Okay. Quickly then, here is the PCCIP (figure 10). Since you have read the report, I will assume you have some familiarity with this. This commission, in my view, was given a very broad responsibility and broad charter and was pressed to be able to accomplish all the things that it was instructed to accomplish in a very short period of time. You can question Tom Marsh about that.

PDD 63 was supposed to implement such of the findings and recommendations of the PCCIP as the President deemed to be worthy of implementation (figure 11). In my view, the most important thing in this PDD is that for the first time in national policy we have a goal, stated by the President of the United States, to protect the infrastructures from intentional acts. That has been set out. It is important in the evolution of policy that this will be a marker. It emphasizes the importance of public and private cooperation that we have spoken about, and then it directs each sector to produce a plan. Sectors are those various infrastructures with lead agencies. So, for example, for energy distribution, the sector lead is the Department of Energy, not surprisingly; or for banking and finance, the sector lead is the Department of the Treasury, and so forth.

The PDD purports to establish a structure to coordinate all of this, and then it directs the NSC principals (basically at the cabinet level) to submit a schedule, and to implement a national plan to integrate the various sector plans for infrastructure protection that have been put together. Those are the essential parts of the PDD.

It also created new players in the infrastructure protection arena, such as the NIPC at the FBI (figure 12). We're not going to have time, I suspect, to get into some of the specifics about the NIPC, but I did leave

- Increasing dependence
- Increasing vulnerability
- Wide-spectrum threat
- Lack of awareness
- No national focus

---

***Shared responsibility***

**Figure 10**
**PCCIP Findings**

- Declares national goal: the ability to protect infrastructures from intentional acts
- Emphasizes importance of public-private cooperation; directs each sector to produce a plan
- Establishes structure for coordination
- Directs NSC principals to submit a schedule to implement a national plan that integrates sector plans

**Figure 11**
**PDD 63**

- NIPC at FBI: provides assessment, warning, vulnerability analysis, law enforcement, response
- National coordinator at NSC: coordinates policy, reviews crisis activities
- National plan coordination staff at DOC: integrates sector plans, coordinates analyses of government dependencies
- Information Sharing and Analysis Center: TBD

**Figure 12**
**PDD 63: New Players**

Tony a copy of the report that our subcommittee did on oversight hearings on the FBI's infrastructure protection center. So for those who are interested specifically in the authorities and who has responsibility, this is a detailed examination.

The PDD also created a national coordinator for infrastructure assurance at the NSC. That individual today is Dick Clarke. He had been assistant secretary of state in the Bush Administration, which is when I knew him, working in the counterterrorism arena, and then moved over to the NSC staff and stayed into the Clinton Administration, where he has been responsible for counterterrorism and crisis management. He has now acquired infrastructure protection as an additional responsibility. The PDD also created a coordination staff in the Department of Commerce, which really supports Dick Clarke, and in addition it said that we need an Information Sharing and Analysis Center that would be created by industry.

This brings us back to the authority of these PDDs, versus that of laws. The PDD can't direct industry, the private sector, or any individual citizen to do anything. The President doesn't have the power to do that; only the duly enacted laws of the country can do that. So they struggled a long time about how to write this so it didn't appear to exceed their authority, and it sort of says, "Gee, it would nice if the private sector would create such a thing because we really need it." So that's what the PDD did, and there are still all kinds of different proposals and different players in the private sector that are interested in participating.

The various responsibilities given to the NIPC are on the next slide (figure 13). The important thing to note about this is the breadth of the responsibilities handed to the FBI. It's interesting, because doing I&W has never been an FBI responsibility. That is an intelligence community function, but it's now vested at the FBI, along with some things likecomputer criminal investigations, which are their mainstream job. However, the FBI has a little difficulty doing other things, such as assessment, training, and outreach in critical infrastructure protection, because if you're a guy who owns a plant and the FBI shows up and says, "Tell me if you have had any intrusions around here, because we'd like to help you about it," you're going to wonder, "Okay, what have I done wrong?" In dealing with a law enforcement agency, the private sector has a bit of a different relationship than it does in dealing with other parts of the government, and this has been something that the FBI has been working on trying to overcome.

The Critical Infrastructure Assurance Office at Commerce (figure 14), which we've already discussed, also has broad responsibilities. The missing player, however, is really the Department of Defense. PDD 63 gives very little responsibility to the DOD, but the assistant secretary of defense for command, control, communications and intelligence (ASD $C^3I$) continues to have responsibility within the DOD organization for offensive and defensive IW. That's not spelled out in the PDD, nor is DISA's responsibility for intrusion detection (figure 15).

| History | | Responsibility |
|---|---|---|
| • Feb. 1992 | FBI computer crime squad | • Computer criminal investigations |
| • June 1995 | PDD 39 (CIWG) | • CIP protection via assessment, training, outreach |
| • Sept. 1995 | NSTL | • Indications and warning |
| • July 1996 | EO 13010, IPTF, CITAC | • Counterintelligence |
| • Dec. 1997 | CITAC becomes NIPC | • Counterterrorism |

**Figure 13**

**National Infrastructure Protection Center**

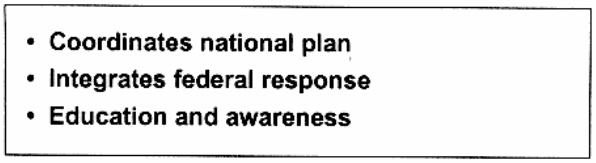



**Figure 14**
**Critical Infrastructure Assurance Office**

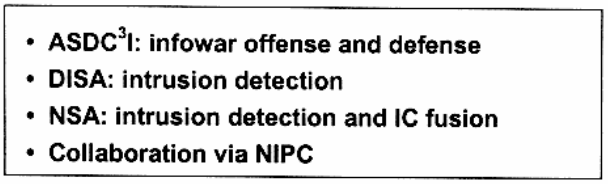



**Figure 15**
**Lead Agencies**

But they have it pursuant to the direction of the secretary of defense. NSA's role in here is also at the direction of the secretary of defense, not spelled out in the PDD.

**Oettinger:** You've heard from those two organizations: Cunningham representing the ASD C$^3$I, and of course General Kelley.[5] Again, you're beginning to see the elephant from several directions.

**Van Cleave:** Here are all the directions at once (figure 16). I have a little anecdote to tell you. We had Dick Clarke come up to brief the committee. (He wasn't formally a witness because, as I explained, NSC staff are exempt from being called to testify. So we worked out a deal where we called it a briefing, but it was all recorded and looked just like testimony.) Senator Dianne Feinstein of California is the senior Democrat on the subcommittee, and she couldn't visualize this organization. She was trying to figure out, "Who does *this* and what does the Commerce group do, and what do you do, and how do you fit into this?" Dick was struggling trying to explain how all this comes together. My staff had put together this little chart. I was sitting behind her, and I said, "Senator, here it is," and she looked at this and said, "Oh, my goodness!" She held it up and she said to poor Dick Clarke, "*This* is the organization you set up?! No wonder I can't understand it! How can anybody understand this? How can this be?"

It is a little bit confusing. You can disentangle it, but there are a lot of players, and a lot of assignments given under PDD 63. I wouldn't care, or I don't think we would care, about the alphabet soup and all of this because it may well be the case—in fact, it is the case—that we need to have a lot of participants doing a lot of things to have a coherent and effective program for infrastructure protection in the federal government. However, the real problem I have is that while PDD has a lot of nouns in it—this office, that office, that entity, and the other entity—it's pretty much devoid of verbs. It doesn't tell whom to do what. It sets up all of these things, and basically the only verb you see is, "*This* group supports *that* group, and *this* group assists *that* group." Other than that, it doesn't assign responsibility, which is a major problem. So I thought you would be interested in seeing that.

Now, mind you, the earlier timeline (figure 8) shows that in 1996 (it was the 1996 DOD authorization bill, so it was really in 1995), Congress, at the initiative of Senator Kyl, first directed that the President report on a national strategy to do these things. It's now four years later, and this is where we are (figure 17). PDD 63 directs that some day there shall be a national plan, and the national plan will do all these things. The national plan will analyze all of our vulnerabilities and recommend how to remedy them. It will design a warning system and a response system. It will design a reconstitution system and ensure that there is an education and awareness program. It will coordinate all R&D. It will direct the intelligence community to enhance collection and analysis of threats. It will figure out how to expand our international cooperation, because all of these networks that are interconnected domestically are also connected to global networks, and it will evaluate legislative and budgetary requirements that fall out of it.

[5] See the presentations by General Cunningham and General Kelley in this volume.

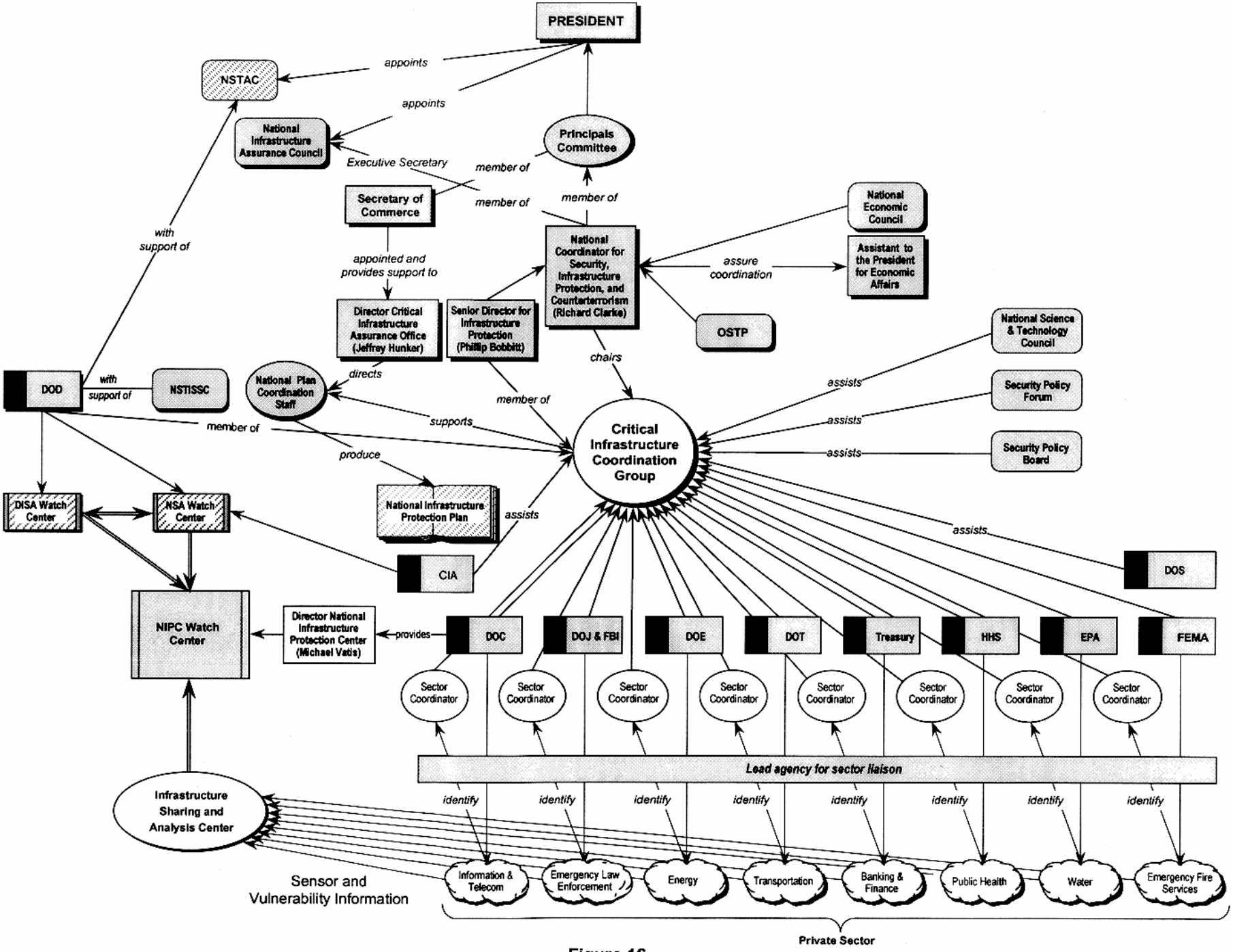



**Figure 16**
**Structure Established by PDD 63**

| | |
|---|---|
| • Vulnerability analysis<br>• How to remedy<br>• Design warning system<br>• Design response system<br>• Design reconstitution system<br>• Awareness and education plan | • Coordinate R&D<br>• Intelligence community to develop plan to enhance collection and analysis of threat<br>• How to expand international cooperation<br>• Evaluate legislative and budgetary requirements |

**Figure 17**

**PDD 63: National Infrastructure Assurance Plan**

This PDD was three years in the making, and it answers none of these issues. It says that some day we have to answer these issues, but it doesn't lay out a plan to do a single one of these things—not a one, after all that time.

So, some of the observations I would make about PDD 63 are that, with its broad language, it lacks specificity (figure 18). We were talking about how you write these PDDs. You are the President, so you don't just say general things. You've got a government you have to run, and you've got limited time, and everybody is out there working. You had better be very specific about what it is you want whom to do, and when you want them to do it, and how you want them to do it. You're directing; that's why these things are called Presidential Decision Directives. You write directive language. This one doesn't. It doesn't define what we're protecting (those three different columns of protection in figure 9), or what we're really doing here. It doesn't define the threat. What is it we're protecting against? It doesn't really say. It just says "intentional acts of disruption," and everything kind of gets thrown into the same bag. Now, let me say, all of those things are important, but they're not dealt with in the same way. You have to be analytically rigorous in how you're dealing with different kinds of threats. This PDD doesn't break it out.

It lacks organizational tasking or resource allocations, which has become an issue because the budget submissions to the Congress have not been supported. Why haven't they been supported? The appropriations committees, in particular, have said, "You've asked for this money, but you can't tell us what you're going to do with it. Request denied." That's been a problem.

It's essential that there be private sector participation for success, but there's really no strategy to engage the private sector, nor is there any explication of what the private sector would be asked to do or why it would be asked to do it. But you have to do it, because

| | |
|---|---|
| • Broad language, lacks specificity<br>• Undefined concepts of protection or threat<br>• Lacks specific organizational tasking or resource allocations<br>• Private sector participation essential for success | • PDD 63 does not:<br>– Address IW threat<br>– Identify elements or assign responsibility for defense against IW attack, e.g., deterrence, counter-IW operations.<br>– Establish an I&W architecture.<br>– Establish a process to identify what is critical<br>– Provide a foreign counterintelligence strategy for IW protection. |

**Figure 18**

**PDD 63 Analysis**

companies sitting back there are going to say, "Hey, I'm prepared to do what I have to do, but I want to know that if I do it it's going to be useful and have a purpose."

This PDD (I encourage you to read it) doesn't talk about the IW threat at all. It's not mentioned. It doesn't identify the elements of what a defensive strategy would look like, or assign responsibility for those things. For example, you have different phases of concern in thinking about the IW problem. You have the day-to-day kinds of assurance activities; you have the kinds of things that have to be done in building up to a crisis of some kind; you have the specific actions that need to be taken in the event that you're in a crisis situation, including counterinformation operations; and then you have reconstitution and recovery responsibilities.

There are ways of figuring out analytically what needs to be done, and then once you've figured that out, assigning responsibility for coming up with a plan to do these things. But this PDD doesn't identify the elements of a strategy to protect the infrastructure, and not having identified the elements, it can't assign responsibility for any of those elements. It doesn't do anything about I&W. It simply says, "The FBI is responsible for warning," but the FBI has no experience or resources to be able to do the warning mission. If we had more time, and another opportunity, I've done a lot of thinking and actually have another briefing on what an I&W architecture would look like for a strategic IW attack. It's very stressing, and it's very complicated, and it's not something that you would ask the FBI to do if you were really serious about this. You need to set up a much more thoughtful and comprehensive architecture, instead of just saying, "We'll get Mikey to do it, because Mikey likes everything."

It doesn't establish a process to identify what is critical, something we were talking about earlier. Not everything is of equal criticality. Setting up the process for doing risk management with respect to these national infrastructures is not a small undertaking, but it needs to be done.

It also doesn't provide a foreign counterintelligence strategy for IW protection. Leaping into the question of what a strategy might look like, it is my guess that the resources that would be devoted to denying potential adversaries the vital information and access they would need to be able to carry out an effective IW attack against the infrastructure may be the highest-leverage resources we have. It may be that a deterrent strategy may not work because you've got such a variety of actors that could be players in the IW attack arena, so your resources and effort for deterrence might not be as effective as a strategy that would generally deny access or information and would protect, in a counterintelligence way, those things that are most vital. It's a question.

**Oettinger:** It's also one on which it's counter to my self-interest to stop you at this point, but we promised to get you on an airplane back. With that in mind, I must bring it to a halt and thank you for an excellent presentation. You set yourself up for seeing us next year. But before that, thank you so much. Here is a token of our big appreciation.

**Van Cleave:** Isn't this nice? Thank you, that's lovely. I have a display case in which this will go nicely.

INCSEMINAR1999

ISBN-1-879716-63-1