

# **AFCEA TechNet '98 Fort Monmouth**

---

## **Vulnerabilities and Threats & US Government Response**

**New Jersey**

**September 1998**

•

**Mike McConnell**

**Vice President, Booz-Allen & Hamilton**

## Form SF298 Citation Data

<b>Report Date</b> <i>("DD MON YYYY")</i> 00091998	<b>Report Type</b> N/A	<b>Dates Covered (from... to)</b> <i>("DD MON YYYY")</i>
<b>Title and Subtitle</b> Vulnerabilities and Threats & US Government Response		<b>Contract or Grant Number</b>
		<b>Program Element Number</b>
<b>Authors</b>		<b>Project Number</b>
		<b>Task Number</b>
		<b>Work Unit Number</b>
<b>Performing Organization Name(s) and Address(es)</b> Booz-Allen & Hamilton		<b>Performing Organization Number(s)</b>
<b>Sponsoring/Monitoring Agency Name(s) and Address(es)</b>		<b>Monitoring Agency Acronym</b>
		<b>Monitoring Agency Report Number(s)</b>
<b>Distribution/Availability Statement</b> Approved for public release, distribution unlimited		
<b>Supplementary Notes</b>		
<b>Abstract</b>		
<b>Subject Terms</b>		
<b>Document Classification</b> unclassified		<b>Classification of SF298</b> unclassified
<b>Classification of Abstract</b> unclassified		<b>Limitation of Abstract</b> unlimited
<b>Number of Pages</b> 17		

<b>REPORT DOCUMENTATION PAGE</b>			<i>Form Approved OMB No. 074-0188</i>
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.			
<b>1. AGENCY USE ONLY (Leave blank)</b>	<b>2. REPORT DATE</b> 9/25/87	<b>3. REPORT TYPE AND DATES COVERED</b> Briefing	
<b>4. TITLE AND SUBTITLE</b> Vulnerabilities and Threats & US Government Response		<b>5. FUNDING NUMBERS</b>	
<b>6. AUTHOR(S)</b> Mike McConnell			
<b>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</b> IATAC Information Assurance Technology Analysis Center 3190 Fairview Park Drive Falls Church VA 22042		<b>8. PERFORMING ORGANIZATION REPORT NUMBER</b>	
<b>9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)</b> Defense Technical Information Center DTIC-IA 8725 John J. Kingman Rd, Suite 944 Ft. Belvoir, VA 22060		<b>10. SPONSORING / MONITORING AGENCY REPORT NUMBER</b>	
<b>11. SUPPLEMENTARY NOTES</b>			
<b>12a. DISTRIBUTION / AVAILABILITY STATEMENT</b>		<b>12b. DISTRIBUTION CODE</b>  A	
<b>13. ABSTRACT (Maximum 200 Words)</b> This AFCEA briefing outlines information vulnerabilities and threats and the US Government response. The briefing discusses the trends in the information age, data protection over time, the evolving defense environment, threat awareness over the past, present and future, and PDD-63.			
<b>14. SUBJECT TERMS</b> Vulnerabilities, data protection		<b>15. NUMBER OF PAGES</b>	
		<b>16. PRICE CODE</b>	
<b>17. SECURITY CLASSIFICATION OF REPORT</b> Unclassified	<b>18. SECURITY CLASSIFICATION OF THIS PAGE</b> UNCLASSIFIED	<b>19. SECURITY CLASSIFICATION OF ABSTRACT</b> UNCLASSIFIED	<b>20. LIMITATION OF ABSTRACT</b>  None

# Information Age Trends

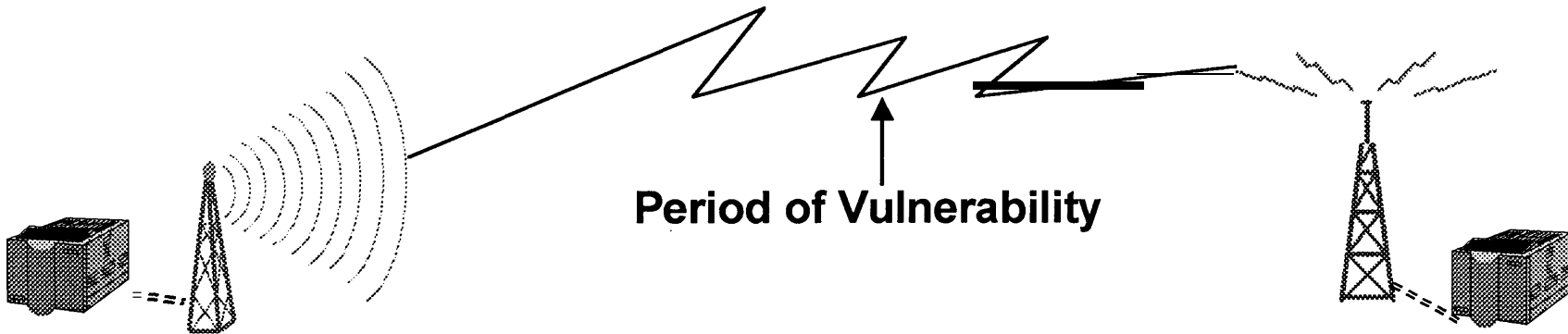
---

- **INFORMATION has become the Primary Capital (Human Intelligence & Intellectual Capital)**
- **Instant Global Communications & Networking have Profound Consequences**
- **Public & Private Institutions and markets will be transformed**
- **National Boundaries are increasingly irrelevant**
- **Traditional Power & Perquisites of Sovereignty are Disappearing (In govt and private organizations)**
- **Vulnerability of Networked Information has increased**

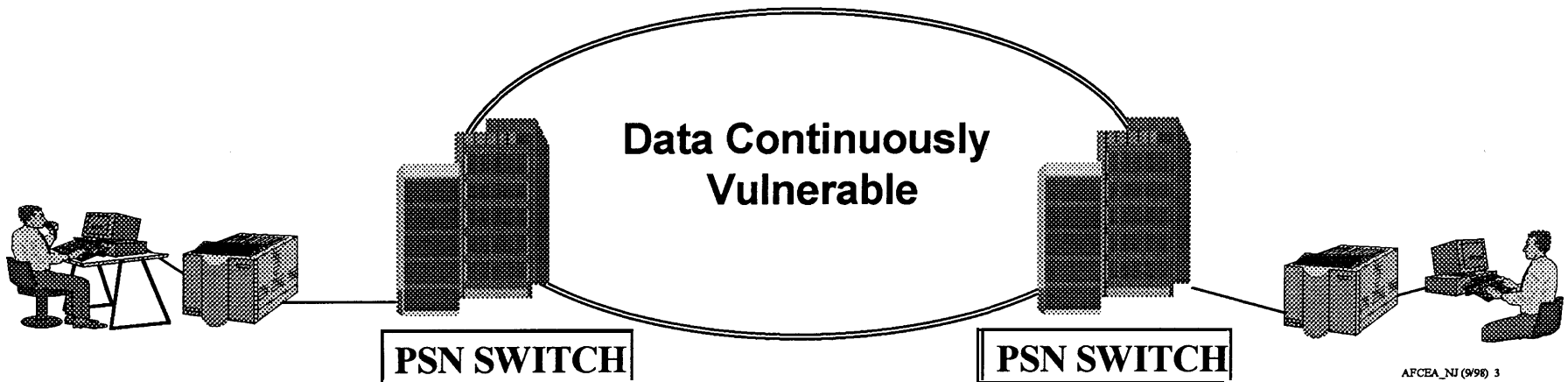
# Data Protection Yesterday & Today

---

## Data in Motion



## Data in Motion *AND* at Rest



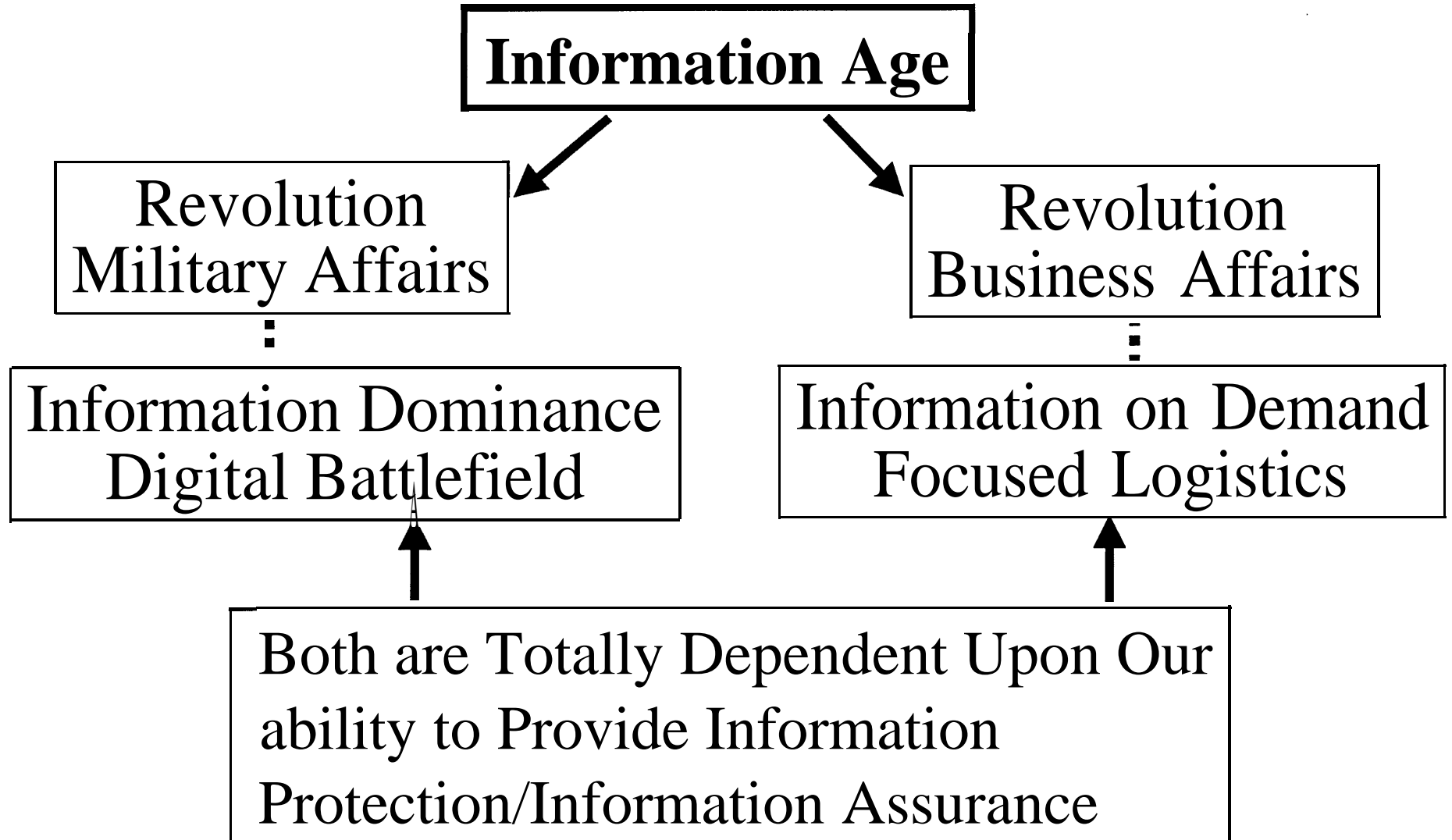
# How Vulnerable Are We?

---

- **Massive Networking makes the US. the *World's Most Vulnerable Target* for Information Attack**
  - **Exploitation (Passive)**
  - **Disruption of Network Infrastructure (Theft-Destruction)**
- **U.S. has *Orders of Magnitude More To Lose* than other nations**
- **Reliance on Unprotected Networks carries *Risk of Military Failure, Catastrophic Economic Loss, Damage to Critical Infrastructures***

# Evolving Defense Environment

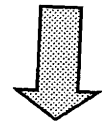
---



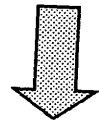
# Risk Equation

---

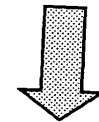
$$\text{Vulnerabilities} \times \text{Threats} = \text{Risks}$$



**Known**



**Less  
Known**



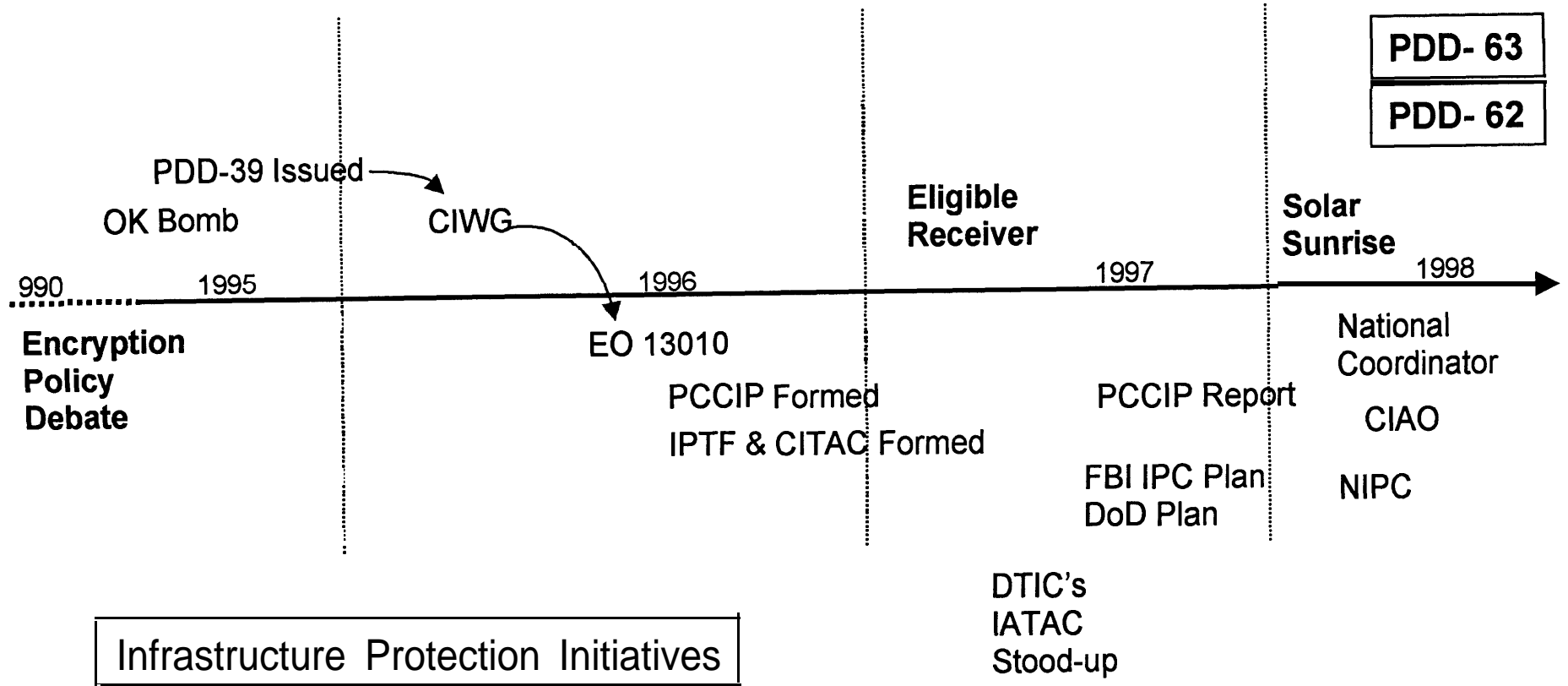
**Least  
Understood**

# **Threat Awareness Past/Present/Future**

---

- **Govt/Media Reports of Vulnerabilities 1993-96**
- **PDD-35, PDD-39 (Intelligence Priorities/Counter-Terrorism)**
- **Executive Order (EO) 13010 (PCCIP)**
- **Economic Espionage Act 1996**
- **Defense Science Board (DSB) IW-D Report - Nov 96**
- **Executive Order (EO) 13026 - Nov 96 (Encryption Policy)**
- **Senate Secrecy Commission - Mar 97**
- **Presidential Commission (PCCIP) Recommendations Oct 97**
- **PDD-63 (Critical Infrastructure Assurance) - May 98**
- **National Infrastructure Assurance Plan - May 2000**

# Infrastructure Assurance Timeline ...



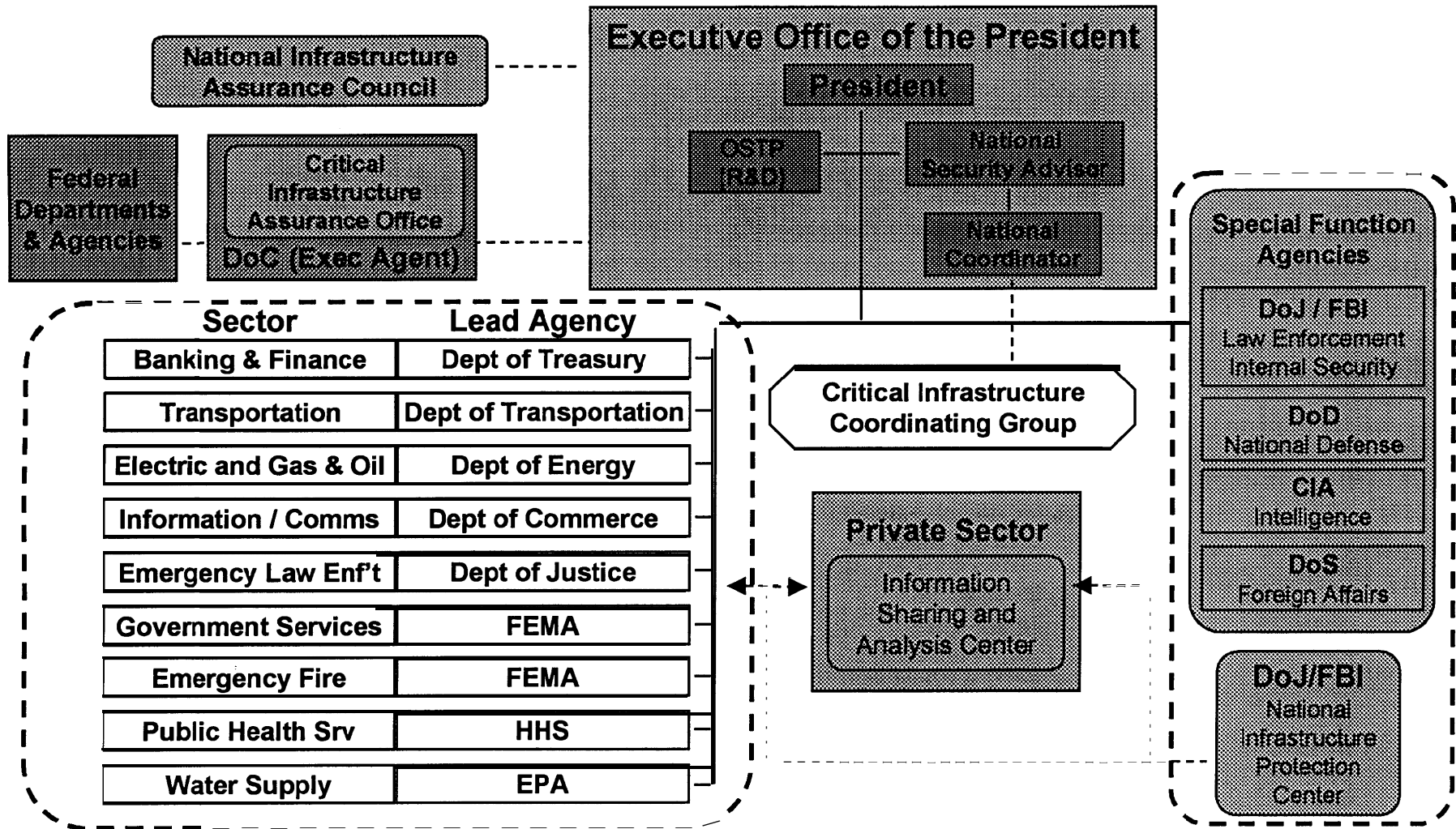
# **PDD 63**

## **Vulnerability & President's Intent**

---

- . President's Recognition of "Growing Potential Vulnerability"**
  - Critical Infrastructures linked and interdependent**
  - U.S. heavily reliant upon networked systems**
  - Cyber threat is real**
  
- . President's Intent: "U.S. will take all necessary measures.. ."**
  - To eliminate any significant vulnerability to U.S. physical or cyber attacks on our critical infrastructures**

# PDD-63 Organization



# **PDD 63**

## **Public-Private Partnership**

---

- **Since critical infrastructures are mix of public-private stakeholders, elimination of potential vulnerability requires closely coordinated effort between public and private sector**
  - **To succeed, must be “genuine, mutual and cooperative”**
  - **Avoid, where feasible, increased government regulation and unfunded mandates**
  - **Appoint Sector Liaison to work with private industry Sector Coordinator**

# **PDD-63**

## **Every Department / Agency ...**

---

- **Shall be responsible for protecting its own critical infrastructures**
- **CIO will be responsible for Information Assurance**
- **Shall appoint a Critical Infrastructure Assurance Officer (CIAO) responsible for protection of all the other aspects of that department's critical infrastructure**
- **Develop a plan for protecting its own critical infrastructure, no later than 180 days from the PDD**

# **PDD 63**

## **National Infrastructure Protection**

---

- . By 2003 achieve ability to protect nation's critical infrastructures from intentional acts that would diminish the ability of:**
  - The Fed govt to perform essential national security missions and ensure the public health and safety**
  - State & Local governments to maintain order and to deliver minimum essential public services**
  - The Private Sector to ensure the orderly functioning of the economy & the delivery of essential telecomm, energy, financial, and transportation services**

# **PDD-63**

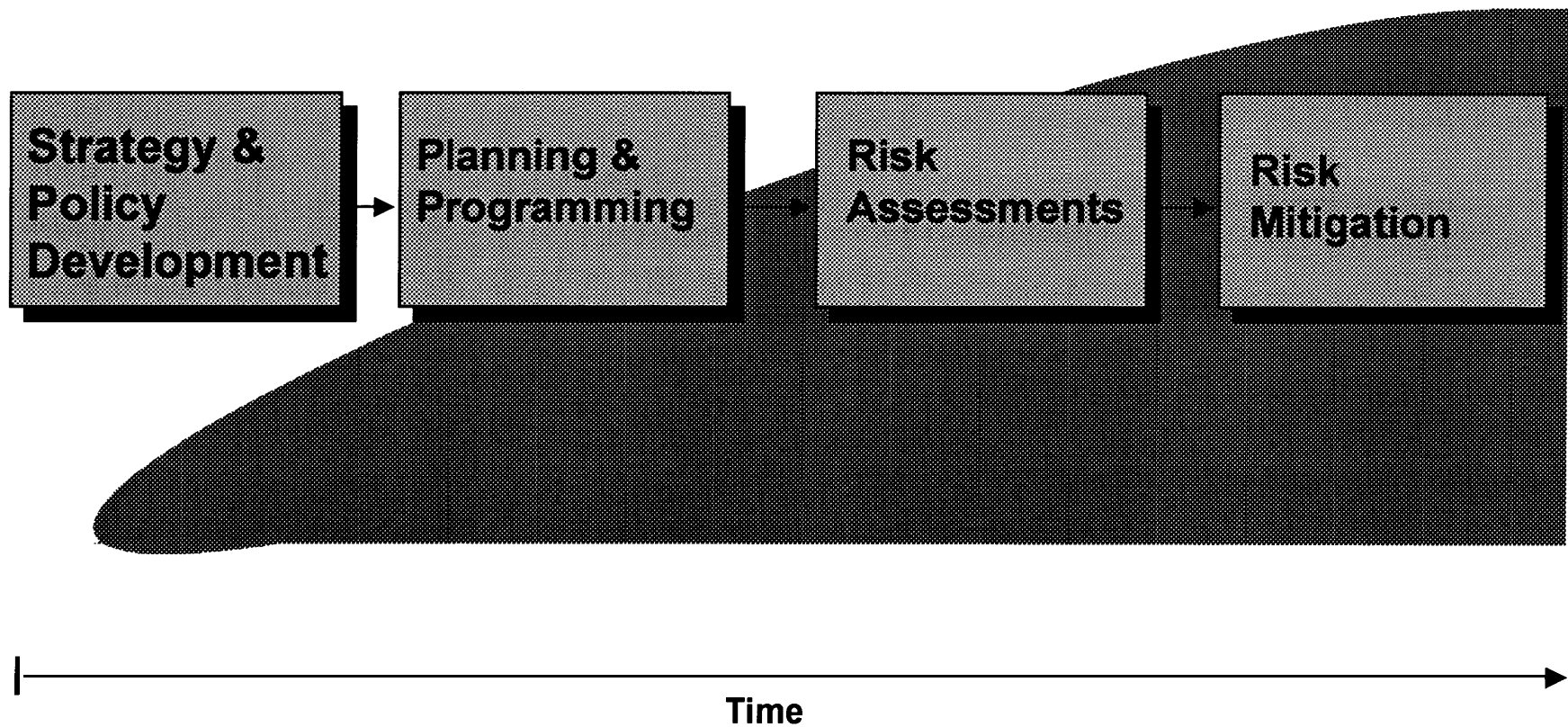
## **Task Areas**

---

- Vulnerability Analyses**
- Remedial Plan**
- Warning**
- Response**
- Reconstitution**
- Education & Awareness**
- Research & Development**
- Intelligence**
- International Cooperation**
- Legislative & Budgetary Requirements**

# PDD-63 Requirements

---



# **“At the end of the day,...”**

---

- **Vulnerabilities**
  - Real but not Widely Recognized
  - Governments Just Beginning to Focus
  - Industry is Not Focused on this issue
- **Threat**
  - Real, but Difficult to Quantify
  - Government is Changing Focus from Traditional Threat to Information Age Threat
  - Industry Barely in the Acceptance Stage
- **Risks Exist But**
  - Understood by Only a Small number of People
  - Government - Still Trying to Define
  - Industry - Nowhere near Consensus