Vulnerabilities and Threats
& US Government Response

New Jersey
September 1998

Mike McConnell
Vice President, Booz-Allen & Hamilton
**Form SF298 Citation Data**

<table>
<thead>
<tr>
<th>Report Date</th>
<th>Report Type</th>
<th>Dates Covered (from... to)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(&quot;DD MON YYYY&quot;) 00091998</td>
<td>N/A</td>
<td>(&quot;DD MON YYYY&quot;)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title and Subtitle</th>
<th>Contract or Grant Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerabilities and Threats &amp; US Government Response</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Authors</th>
<th>Project Number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Task Number</td>
</tr>
<tr>
<td></td>
<td>Work Unit Number</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Performing Organization Name(s) and Address(es)</th>
<th>Performing Organization Number(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Booz-Allen &amp; Hamilton</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sponsoring/Monitoring Agency Name(s) and Address(es)</th>
<th>Monitoring Agency Acronym</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Monitoring Agency Report Number(s)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Distribution/Availability Statement</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved for public release, distribution unlimited</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Supplementary Notes</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Abstract</th>
<th></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Subject Terms</th>
<th></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Document Classification</th>
<th>Classification of SF298</th>
</tr>
</thead>
<tbody>
<tr>
<td>unclassified</td>
<td>unclassified</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Classification of Abstract</th>
<th>Limitation of Abstract</th>
</tr>
</thead>
<tbody>
<tr>
<td>unclassified</td>
<td>unlimited</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number of Pages</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td></td>
</tr>
</tbody>
</table>
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.
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

Period of Vulnerability

Data in Motion AND at Rest

Data Continuously Vulnerable

PSN SWITCH

PSN SWITCH II
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

Information Age

Revolution
Military Affairs

Information Dominance
Digital Battlefield

Both are Totally Dependent Upon Our
ability to Provide Information
Protection/Information Assurance

Revolution
Business Affairs

Information on Demand
Focused Logistics
Risk Equation

Vulnerabilities $\times$ Threats = Risks

$K_{\text{Known}}$

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...

- Encryption Policy Debate
- PDD-39 Issued
- OK Bomb
- CIWG
- EO 13010
- PCCIP Formed
- IPTF & CITAC Formed
- Eligible Receiver
- Solar Sunrise
- 1990
- 1995
- 1996
- 1997
- 1998

- National Coordinator
- CIAO
- NIPC
- FBI IPC Plan
- DoD Plan
- PCCIP Report
- DTIC's
- IATAC
- Stood-up

Infrastructure Protection Initiatives
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
Since critical infrastructures are a 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

Strategy & Policy Development → Planning & Programming → Risk Assessments → Risk Mitigation

Time
"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 theAcceptance Stage

- **Risks Exist But**
  - Understood by Only a Small number of People
  - Government - Still Trying to Define
  - Industry - Nowhere near Consensus