Smart Grid: The Rest of the Story

(Part 12)

Emergency!

.....This is 911.... What is your emergency?

In 1950, the <u>National Security Resources Board</u> submitted a report to President Harry Truman which described a plan to create a Civil Defense Administration and to write a basic civil defense law. The plan was based on the wartime experience of Great Britain and Germany. It was written by Russell Hopley who said in a letter to Secretary Forrestal:

"In the event of a future war, which might come to our shores, all of the people, all of the facilities, and all of the skills and energies of the Nation must be utilized to the fullest extent. To successfully carry out this program will require the cooperation of every man, woman and child in this Nation. It is on such principles that civil defense must be erected and it must be with such a requirement that its organization be perfected".

The plan defines "The most important goal of the Government and the community is the prompt, orderly restoration of normal community life, thereby preserving maximum civilian morale and support for the war effort".

In 1979, following the earlier reorganization of government (Energy and Senior Executive Service), the Cult of Doom President Jimmy Carter created the Federal Emergency Management Agency (FEMA) by issuing Executive Order 12127. The new agency included Defense Civil Preparedness Agency which had its genesis in the Truman era Civil Defense Administration. http://www.fema.gov/about-agency John Macy was named as the first director. He set the direction for the agency to develop an "integrated Emergency Management System with an *all-hazards approach*. This approach encompassed direction, control and warning systems".

ALL HAZARDS: floods, fires, drought, alien from space invasion, planetary collision, pandemic infection, war, etc. It also included the planning for **Continuity of Government** which became known to the public during a hearing when <u>Senator Jack Brooks</u> attempted to question Oliver North about it.

Communications

"In 1957, the National Association of Fire Chiefs recommended creation of a single phone number to be used to report fires. In 1967, the President's Commission on Law Enforcement... recommended the creation of a single number that could be used nationwide for reporting emergencies. ...In 1968... AT&T implemented the concept using the number 9-1-1.

Due to communications difficulties during the Cuban missle crisis in 1963, and following a study of national security communications, President John F. Kennedy established the National Communications System (NCS) by Presidential Memorandum on August 21, 1963. "The mandate included linking, improving and extending the communications facilities and components of various Federal agencies focusing on interconnectivity and survivability".

From the NCS website – emphasis added:

The text in the boxes are excerpts from NCS – NSTAC – web archive

"President Ronald Reagan created the National Security Telecommunications Advisory Committee (NSTAC) by Executive Order 12382 in September 1982. Since then, the NSTAC has served four presidents. Composed of up to 30 industry chief executives representing the major communications and network service providers and information technology, finance, and aerospace companies, the NSTAC provides industry-based advice and expertise to the President on issues and problems related to implementing national security and emergency preparedness (NS/EP) communications policy."

The published membership list of the NSTAC Council along with their Industry Executive Subcommittee (IES) appointees for 2004 was captured from the Internet archive. The following is a list of the corporations involved:

National Security Telecommunications Advisory Committee (NSTAC)

Bellsouth Lucent
Unisys Boeing
Microsoft SBC
Northrup Grumman Qwest
AT & T SAIC

Bank of America Cingular Wireless (CTIA)
Lockheed Martin D&E Telephone Company

Electronic Data Systems (EDS)

Advanced Micro Devices, Inc.

Computer Sciences Corporation (CSC)

Sprint

MCI

Verisign

Motorola Rockwell Collins, Inc. (Rockwell Intl.)

Nortel Networks Verizon
Teledesic Raytheon

PanAmSat

NCC = National Communications Center; ISAC = Information Sharing and Analysis Center

Telecom-ISAC:

The NCC was established in 1984 as a result of an NSTAC recommendation to develop a joint government-industry national coordinating mechanism to respond to the Federal Government's NS/EP communications service requirements. The NCC's mission is to assist in the initiation, coordination, restoration and reconstitution of NS/EP communications services or facilities. Currently 13 NSTAC member companies are represented in the NCC. The NSTAC was instrumental in expanding the NCC's responsibilities to include functioning as an ISAC for the telecommunications

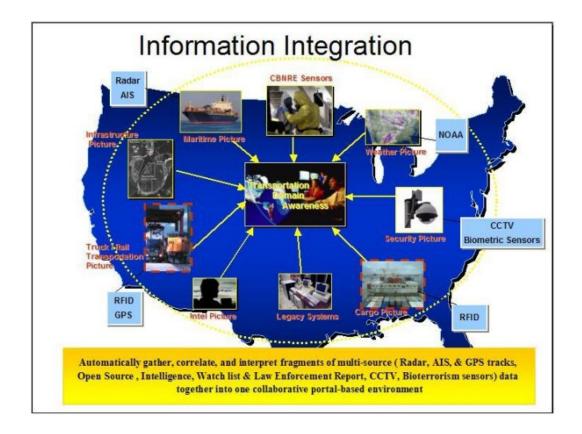
infrastructure. Established in January 2000, the NCC-ISAC was the second ISAC to be formed following the promulgation of Presidential Decision Directive 63 (PDD-63) and the first ISAC with both industry and Government membership. The NCC-ISAC gathers information about vulnerabilities, threats, intrusions, and anomalies from telecommunications industry, Government, and other sources, and then analyzes the data with the goal of averting or mitigating effects on the communications infrastructure. Results are sanitized and disseminated in accordance with sharing agreements established by the NCC-ISAC participants.

National Security Information Exchange (NSIE):

In 1991, the NSTAC, working with the OCS, recommended establishing a Government-industry partnership to reduce the vulnerability of the Nation's telecommunications systems to electronic intrusion. The Octobration Exchange (NSIE) process was established as a forum in which Government and industry could share information in a trusted and confidential environment. The NSIE process continues to function today, demonstrating that industry and Government will share sensitive security information if they find value in doing so. In 1998, PDD-63 called for the establishment of similar information exchange forums to reduce vulnerabilities in all critical infrastructures.

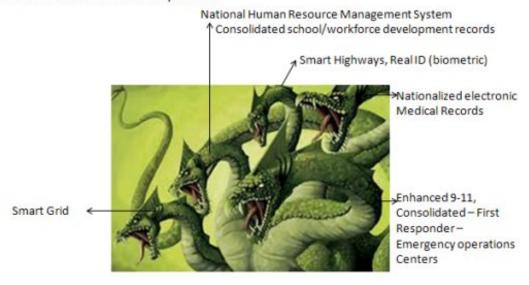
In earlier research, <u>1991</u> was identified as the pivotal year for transformation of the United States to a police state control grid with corporations injecting their business objectives into a full spectrum dominance matrix of control and information gathering and sharing. The cold war ended and the <u>defense contractors were repurposed</u> to develop weaponized infrastructure and surveillance and tracking systems for domestic and global use.

The research on the NAFTA Superhighway — the existence of which was denied by media and our representatives in Congress until the I-35 corridor toll road plan was revealed, it was discovered that full spectrum domain dominance in the form of surveillance and tracking technology and systems was designed between 1988 and 1991. It originated with a transportation plan in Texas called Mobility 2000. With the passage of the High Performance Computing Act of 1991 and the Intermodal Surface Transportation Efficiency Act of 1991, the American Stasi was born. What precipitated this technological surge was the supposed collapse of the Soviet Union and the taking down of the Berlin Wall. In retrospect, it was like the passing of the token ring.



The consolidation of information systems into an enterprise architecture with consolidated information systems began with the systems on the right hand side and progressed toward the design and inclusion of the nation's electric grid – laden with technology for centralized command and control.

To name a few heads of the beast systems...



* Not all of these systems were announced and they didn't arrive immediately after 1991 but all of them derive from the capabilities enabled by the NCS/NSTAC fascist partnership between government and private enterprise behind the cover of national security and emergency preparedness. In June of 1999, NSTAC produced a telecommunications advisory: <u>The Information Infrastructure</u> <u>Group Report</u> that included the following on page 13 and 14:

3.5.1 Analysis

With the PDD-63 emphasis on public-private partnerships, the IIG focused on sharing the lessons and successes of NSTAC and offering it as a possible model for other infrastructures. In particular, IIG members coordinated with Federal officials responsible for the following initiatives:

 Sector Coordinators. PDD-63 directs Federal Lead Agencies to identify a Sector Coordinator to represent the industry perspective on IA/CIP programs. At NSTAC XXI in September 1998, the NSTAC's Operations Support Group reported its conclusion that more than one entity would be required to represent the diverse Information and Communications sector. Since then, IIG members have met with officials from the Department of Commerce, the Lead Agency for the Information and Communications sector. In February 1999, the Department of Commerce acted

in concert with NSTAC's advice and selected three organizations (Information Technology Association of America, Telecommunications Industry Association, and United States Telephone Association) to serve as the Sector Coordinator for the Information and Communications sector.

The CEO of the Information Technology Association of America (ITAA) was a guy named **Harris Miller**, **an immigration attorney**. The Secretary of Commerce at the time was William M. Daley – of Chicago.

Keeping in mind, that the whole entire reason for NSTAC was because of the sensitive nature of both public and private computer systems, there is only one reason for an organization like ITAA and Harris Miller to be included. It was because it was part of the strategy for a coup d'etat because presumably, a background check would have been performed on Harris Miller before he was allowed to be engaged in any activity having to do with national security. QED

Before I was aware of any of this information concerning the National Communications System, alleged infrastructure protection or any of it, I did my own <u>background check on Harris Miller</u> because he was the leading proponent of outsourcing and the importation of Indian IT people to work on American IT systems. Finding out that this dirtbag was selected to be a sector coordinator on anything to do with national security and infrastructure protection reveals the entire program to be a fraud and all the people involved with it to be potential "terrorists on the inside". The following are quotes from what I wrote – based on the research I did on Harris Miller between 2004 and 2005:

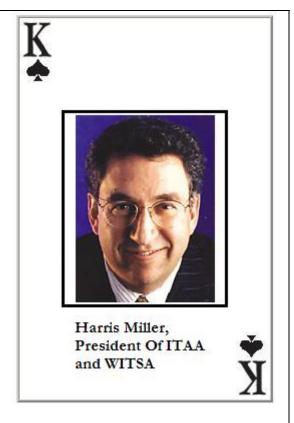
Harris Miller has orchestrated the destruction of our economy by working both sides of the ocean. Initially, the export of our high technology jobs was done in secret as explained by WIPRO Chairman Azim Premji while "speaking at a seminar organised by the All India Management Association (AIMA) and Bombay Management Association (BMA)". [3]

"Addressing management students here, Mr Premji explained that when software services were being outsourced, it was done surreptitiously. This was done because it was the requirement of that time. The industry then stood witness to a vast number of layoffs."

We know that Harris Miller orchestrated the stealth attack on our economy because of a quote from Dewang Mehta, the "Father of India IT" [4]. In March of 2001 at a signing ceremony of a Memorandum of Understanding (MoU) between NASSCOM and ITAA:

"According to Mr Mehta, Nasscom and ITAA have been working very closely together for the last five years" [5]

Unfortunately, less than a month after making this statement, poor Mr. Mehta, only 38 years old, was found dead in his hotel room - died of a surprise heart attack while attending an IT conference in Australia [6]



That would put the timing for the start of the Indian takeover of our high technology sector at about 1996 shortly after Miller went to work for ITAA. Not coincidently, this was about the same time that the media frenzy was starting over the dot.com boom and the Y2k date rollover problem. The dot.com boom - later called tech bubble ^[7]), with a few notable exceptions, was a fraud ^[8]. The boom turned to bust virtually overnight in the spring of 2000. In hindsight, the boom served a number of purposes that served the financial interests to the tune of billions of dollars for the tech corporations that Miller represents....

Until 1998, the United States had an annual cap of 65,000 H1-Bs, but Congress increased the number to 115,000 for 1999 and 2000. In 2001, the number of H1-Bs is scheduled to drop to 107,500. The cap is set to return to 65,000 in 2002, but industry groups like the Information Technology Association of America are lobbying for more H1-Bs. "We're so far from the equilibrium of the labor market that it's hard to know how much we'll need (H1-Bs), or how long (the demand will) last," said Harris Miller, president of Information Technology Association of America in Washington, D.C. "Every indication is that the demand will grow faster than the supply side."

It should be noted, that there was a "bug" in the computer system that kept track of the H-1B visa applications and a form that held the names of multiple visa applicants was counted as one for the purposes of charging against the national cap.

Put these things together.... critical infrastructure protection with Harris Miller and the ITAA as a sector coordinator and William Daly as the Secretary of Commerce... and the systems to "protect" the critical infrastructure are police state, command, control and surveillance and foreigners are being imported to both work on these systems and run them.

Backtracking once again to the Clinton Administration when all of this was set up, in 1995, Clinton signed Executive Order 12968. Section 2.4:

Sec. 2.4. Reciprocal Acceptance of Access Eligibility Determinations.

(a) Except when an agency has substantial information indicating that an employee may not satisfy the standards in section 3.1 of this order, background investigations and eligibility determinations conducted under this order shall be mutually and reciprocally accepted by all agencies.

The significance of this reciprocity order should be obvious. Turn one agency head – and in particular, in the area of IT and communications, and it becomes a pipeline for traitors and insurgents to all other agencies of government. Adding to that:

The Indians had a substantial number of the members of Congress in their pocket: India PAC

And substantial media support: India Takeover - Media Support

And it was the Clinton Administration that set it up – leaving George W. Bush holding the bag:

Administrative Coup d'etat

<u>USINPAC</u> - Meeting in Washington, September 24, 2003: "The mission you have started has to succeed".

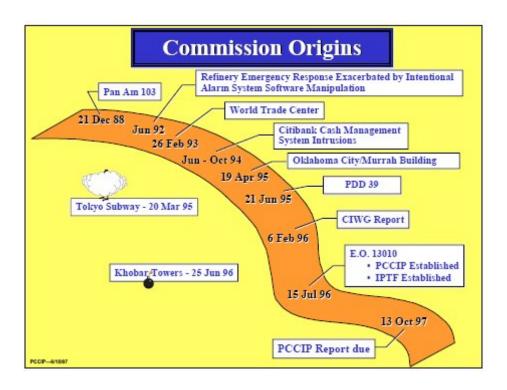
And it should be noted that while Indians and other foreigners have essentially taken over our university graduate programs, our schools - K-12 and junior college are being converted to vocational training: Reinvention of American Education to make America's Children Stupid and incapable of operating the systems of the technocratic tyranny.

The Timeline Tell

Recalling PDD-63, signed in 1998, mentioned above as the directive to establish a "National Security Information Exchange". It was titled *Protecting America's Critical Infrastructure*. PDD-62 was signed on the same day. It was titled *Combating Terrorism*.

The reason given for protecting critical infrastructure was because of the following chain of "terrorist events":

President's Commission on Critical Infrastructure Protection





In May of 2000, the President's National Security Telecommunications Advisory Committee (NSTAC), *Information Sharing for Critical Infrastructure Protection Task Force* report included the following:

As part of IS/CIP Task Force PDD-63-related outreach efforts, members, representing their individual companies, provided support to the Partnership, a collaborative effort of industry and Government to address risks to the Nation's critical infrastructures and assure the delivery of essential services over those infrastructures.

The Partnership was envisioned to provide a forum for the critical infrastructures to exchange views on interdependencies, threats, work-force development, standards and best practices, technology, research and development (R&D), risk management, international matters, legal and regulatory matters, and other areas of mutual concern. In addition, the Partnership would facilitate industry participation in the National Plan process and provide a vehicle for coordinating industry contribution to the work of the NIAC, which was to be established to advise the President on infrastructure assurance and Partnership issues.

Several NSTAC member companies were represented on the steering group organized to provide advice and help facilitate CIAO efforts to form the Partnership. By leveraging the positive experience of the NSTAC, NSTAC members helped shape this new initiative. NSTAC member companies were instrumental in developing the message tailored to areas of importance to industry—fiduciary responsibility and market influences—that eventually became the foundation of the Partnership. In addition, NSTAC member companies worked to increase awareness throughout industry regarding the Partnership.

The initial Partnership event was held at the World Trade Center, New York, on December 8, 1999. Ninety-one attendees representing more than 55 companies and 7 Government organizations joined together to begin a collaborative effort to ensure the delivery of essential services over the Nation's critical infrastructures. Sixteen NSTAC member companies participated. Several pertinent industry points of view were shared with Government, and awareness of network security issues was raised among all eight of the critical infrastructure sectors identified in PDD-63.

So, when the government tries to tell you that the smart grid system is to protect the electric grid from terrorism... you should now understand that it's not true. If any of the systems to control our critical infrastructure had anything to do with national security, there wouldn't be foreigners involved in building and running them while American IT people were pushed out and discarded.

American's Betrayed

For more information on the Fusion Centers which are the NCC ISAC collector and feeder systems, click on this link: Fusion Centers

Vicky Davis August 21, 2014