

TESTIMONY OF  
STANLEY BORGIA  
ASSOCIATE DIRECTOR OF COUNTERINTELLIGENCE  
OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE  
U.S. DEPARTMENT OF ENERGY  
BEFORE THE  
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS  
COMMITTEE OF ENERGY AND COMMERCE  
U.S. HOUSE OF REPRESENTATIVES

September 25, 2008

Chairman Bart Stupak, Ranking Member John Shimkus, and distinguished members of the committee, thank you for the invitation to appear before you on a subject of critical importance: "The Cyber Threat." I am addressing you today as the Deputy Director, Counterintelligence, in the Department of Energy's (DOE) Office of Intelligence and Counterintelligence.

We in DOE Counterintelligence are both a producer of intelligence information, and a consumer of intelligence information. We develop and facilitate the transfer of DOE-unique information to the United States Intelligence Community, and convey actionable Intelligence Community threat information to all Departmental action offices, including NNSA.

We appreciate that physical security is an essential element in the protection of information, and we participate in the National Joint Terrorism Task Force/National Counter Terrorism Center to enhance the protection of DOE equities.

Likewise, we are a very active member of the FBI-led National Cyber Intrusion Joint Task Force, or NCIJTF, which allows us to provide unique DOE and NNSA information to the cyber investigations community and collaborate in national initiatives.

Membership also provides DOE with invaluable current, cyber-based threat information relevant to our own Departmental assets and critical energy infrastructure.

DOE's counterintelligence office performs a broad range of cyber-related functions, including analysis of cyber security incidents with a foreign nexus. Our work is closely coordinated with DOE's Office of the Chief Information Officer (OCIO) and with NNSA's Office of the Chief Information Officer (OCIO), with which we maintain a strong and mutually supportive relationship in the cyber security realm.

The nature of the cyber threat to the DOE complex is constantly evolving. DOE sensors monitoring attacks on the DOE networks have picked up an increased tempo of potential adversarial activity, including network reconnaissance, scanning for potential attack vectors, and outright cyber attacks. In three of the past six months, sensors have documented well over 400 million such indicators of hostile activity every month. Further, we have recently seen thousands of socially engineered e-mails. They may appear to come from known associates or sport an interesting subject line, but they contain malicious computer code designed to infect the recipient's computer, steal and transmit information it contains, and eventually spread to the rest of the network. A single mouse click by a single user can contaminate large numbers of networked computers.

In order to generate counterintelligence investigative leads from all this activity, I have directed expanded use of cyber techniques at DOE and NNSA. The results have been dramatic. In particular, cyber tools developed under this initiative have enabled investigators at intelligence and military organizations to make strides toward attribution for ongoing computer intrusions directed against DOE and other United States Government computer networks—a major accomplishment for DOE that has demonstrated the value of these cyber tools for CI analysis.

The Counterintelligence Cyber Program has developed professional working relationships with the Defense Information Systems Agency, the military service Information Operations Centers, the military service Criminal Investigation Divisions, and the Joint Information Operations Warfare Analysis Center in San Antonio, Texas. These are comprehensive information sharing relationships, as well as expanded partnerships for information and cyber data exchange. They serve to increase awareness of the operational methods being employed by individuals and state sponsored entities engaged in unauthorized computer intrusions into DOE computer networks. DOE—in collaboration with the Intelligence Community partners, DOE National Laboratories, Chief Information Officers and DOE Cyber Security—use data integration tools and intrusion detection sensors, to uncover, investigate, and mitigate suspicious cyber events with a foreign nexus.

In closing, the attacks we see place virtually every computer connected to the Internet at risk of compromise, including those of the U.S. Government and our critical energy infrastructure. Moreover, an attacker has a significant advantage over the "protect and defend" cyber security community. DOE's Office of Intelligence and Counterintelligence will continue to pursue all available lawful means to detect, investigate, and mitigate the pervasive cyber threats we, as a nation, now face.

This concludes my testimony and I look forward to answering any questions you may have.