CRIME - CYBERTERROR

Leanne A. Shimabukuro 02/09/2000 09:08:22 PM

Record Type: Record

To: Bruce N. Reed/OPD/EOP@EOP

cc: Eric P. Liu/OPD/EOP@EOP, Anna Richter/OPD/EOP@EOP, Deanne E. Benos/OPD/EOP@EOP
Subject: Cyber Security

A few things about what I learned today on this:

1. Last month, the President announced a National Plan for Information Protection Services. The announcement originated out of Dick Clark's shop at NSC. The primary focus of the plan is on protecting the federal government's infrastructure from hacking and other threats to security. The press paper describing the plan is below.

2. The report I mentioned to you earlier today was sent to OMB tonight for circulation. The report is a response to an EO signed by the President last August to create a working group on unlawful conduct on the Internet. The report briefly discusses "denial of service" -- the hacking problem in recent reports -- but overall, it is a much broader document that lays out the Internet crime problem and identifies gaps in legal authorities that hinder enforcement. Unfortunately, the report does not make specific recommendations on penalties or legislation. I think its viewed as a "jumping off" document for discussion and later action/proposals. After speaking with Ivan, I think we may be to work with DOJ to squeeze some sort of action to announce out of this document.

Internally, the VP's office has been the lead on the report. Kohlenberger was on the fence about whether this should be released next week if we were to do something to respond to these Internet hacking stories. The other VP contact, Elizabeth Echols, seemed more receptive. I asked OMB to put a short turn-around clearance on the report in case we want to use it next week. I think it makes sense to release it.

3. Our budget contains funding increases to attack cyber crime. The DOJ budget contains a $37 million increase; this number should be higher if we pull together some sort of agency cross-cut.

We can discuss these items further at the staff meeting if there is continued interest in doing an event for next week.

LS

---------- Forwarded by Leanne A. Shimabukuro/OPD/EOP on 02/09/2000 04:51 PM ----------

Christine L. Anderson
01/07/2000 10:41:53 AM

Record Type: Record

To: See the distribution list at the bottom of this message

cc:

Subject: Fact Sheet: President Clinton and Vice President Gore: Promoting Cyber Security for the 21st Century

PRESIDENT CLINTON AND VICE PRESIDENT GORE: PROMOTING CYBER SECURITY FOR THE 21ST CENTURY

January 7, 2000

Today, President Clinton launches the National Plan for Information Systems Protection and announces new budget proposals for initiatives to strengthen America's defenses against the emerging threats posed to our critical infrastructure, computer systems, and networks.

The United States has benefited form the most advanced information technology (IT) infrastructure in the world. This same IT infrastructure, however, makes us particularly vulnerable to cyber attack. The most vital sectors of our economy -- power generation, telecommunications, banking and finance, transportation and emergency services -- are potentially susceptible to disruptions from hackers, terrorists, criminals or nation states. President Clinton has increased funding on critical infrastructure substantially over the past three years, including a 16% increase in the FY2001 budget proposal to $2.03 billion. He has also developed and funded new initiatives to defend the nation's computer systems from cyber attack. To jumpstart the FY01 program initiatives, the President will also propose a $9 million supplemental this spring.

In the 18 months since the President signed Presidential Decision Directive 63, we have made significant progress in protecting our critical infrastructures. Last year the President called for the development of a National Plan to serve as a blueprint for establishing a critical infrastructure protection (CIP) capability. Version One, the "National Plan for Information Systems Protection," was released today. It is called Version One and invites a national dialogue leading to future editions. This plan lays out two broad goals: the establishment of the U.S. government as a model of information security, and the development of a public-private partnership to defend our national infrastructures.

The Federal Government as a Model of Information Security. The Clinton has developed and provided full or pilot funding for the following key initiatives designed to protect the federal government's computer systems:

- *Working to Recruit, Train and Retain Federal IT Experts.* We have developed and provided FY2001 funding for a Federal Cyber ServicesTraining and Education initiative led by OPM and NSF which calls for two programs: the first is an ROTC-like program where we pay for IT education (B.S. or M.S.) in exchange for federal service; and the second is a program to establish competencies and certifyour existing IT workforce. ($25 million)
- *Conducting federal agency vulnerability analyses and developing agency CIP plans.* Federal agencies have all developed CIP plans, and these have been reviewed by a newly created "Expert Review Team" (ERT) of federal computer security experts. We have also established the ERT as a permanent team (at the Commerce Department's NIST), with funding lines in FY2000 and 2001. ($5 million)
- *Designing a Federal Intrusion Detection Network (FIDNET).* To protect vital systems in Federal civilian agencies, we are providing funding for development of a cyber "burglar alarm" which alerts the federal government to cyber attacks, provides recommended defenses, establishes information security readiness levels, and ensures the rapid implementation of system "patches" for known software defects. ($10 million)
- *Piloting Public Key Infrastructure Models.* The Clinton Administration is funding seven PKI pilot programs in FY2001 at different federal agencies. ($7 million)
- *Developing Federal R&D Efforts.* In addition to the Institute, we have worked to ensure that R&D investments in computer security will grow more then 35% in the FY2001 budget. ($621 million)

Building the Public-Private Partnership. The President is committed to building partnerships with the private sector to protect our computer networks through the following initiatives:

- *Institute for Information Infrastructure Protection.* Building on a Science Advisory Panel, we are proposing to create an Information Infrastructure Institute which would combine federal and private sector energies to fill the gaps in critical infrastructure R&D that are not now being meet in the private sector or the Department of Defense. It would also provide demonstration and development support in key areas like benchmarks and standards, and curriculum development. ($50m)
- *Partnership for Critical Infrastructure Security.* This alliance of more than ninety Fortune 500 companies is spearheaded by Secretary Daley and had a successful kickoff in New York on December 8th. We will build on this partnership to provide public education and cooperation with the private sector on a wide variety of information security issues
- *Information Sharing and Analysis Centers (ISACs).* Two of the proposed six private sector computer security centers have been established (banking and finance and telecommunications). We are working with the other four sectors to get their proposed ISACs operational in 2000.
- *National Infrastructure Assurance Council.* The President signed an Executive Order creating this advisory Council, last year. Its members are now being recruited from senior ranks of the IT industry, key sectors of the corporate economy, and academia.

Message Sent To:

CLASSIFICATION
CLASSIFICATION

LOG NUMBER

DRAFT February 9, 2000

Schedule Proposal date____/_____/_____

_____ACCEPT _____REGRET _____PENDING

TO: Stephanie Streett

FROM: Samuel Berger

REQUEST: For POTUS, accompanied by corporate CEOs from Internet companies, Secretary Daley, and Science Advisor Lane, to announce major cyber-security policy initiatives.

PURPOSE: Several major announcements will be made responding to concern about recent Internet 'hacker attacks', and building on the January POTUS release of the National Plan for Information Systems Protection:

1) A group of Internet/computer CEO's and industry leaders (e.g., Cisco Systems, Microsoft, ATT, UUNet, and others) announce the creation of the Cyber-National Information Center (Cyber-NIC), an industry partnership for joint action to solve cyber-security problems and respond to events like the recent hacker disruptions. The Cyber-NIC is voluntary and industry-lead. It builds on Y2K experiences.

2) POTUS announcement of a $9m FY 00 budget supplemental to jump-start key elements of the National Plan: creating an Institute for Information Infrastructure Protection to do R&D to prevent Internet disruptions; launching the Federal Cyber Service scholarship and training programs; investing in protecting Federal computer systems;

CLASSIFICATION
Classified By:
Reason:
Declassify On:
CLASSIFICATION

supporting private sector work to improve cyber-security.

3) POTUS call to:

- Sec. Daley to meet within the week with the Partnership for Critical Infrastructure Security to prepare a plan for additional public-private action to improve security;
- Science Advisor Lane to meet with the President's Council of Advisors on Science and Technology, and other technology experts to advise on needed R&D strategies, including the launching of the Institute;
- Assembled industry leaders to report back on how the Federal government can best assist the Cyber-NIC, and how best can other industries be encouraged to work together in partnership.

BACKGROUND: POTUS has long recognized that computer systems are vulnerable to deliberate attack and intrusion. In May 1998 in PDD-63 he called for a national capability to defend against and recover from such attacks.

On January 7 POTUS released the National Plan for Information Systems Protection, laying out the first-ever national strategy to protect our computer networks from deliberate disruption. It calls for close partnership with US industry, and $2 b in FY01 spending.

Leading up to the Plan release, in December Sec. Daley convened almost 100 major US companies to create the Partnership for Critical Infrastructure Security, a forum for joint industry action to improve cyber-security. Advisor Lane has been working with the PCAST to design the Institute.

On February 8-9, a number of important private sector web-sites were disrupted by hackers. As part of the nationwide publicity and concern about cyber-security, Sec. Daley and AG Reno both gave widely publicized press conferences.

CLASSIFICATION

PREVIOUS PARTICIPATION: Announcement of PDDs 62/63 at Naval Academy commencement, May 1998; January 1999 National Academy of Sciences speech on emerging threats; January 2000 release of National Plan for Information Systems Protection.

DATE AND TIME: ["OPEN" if no specific date/time is given]

BRIEFING TIME: [Time]

DURATION: [e.g. 30 minutes]

LOCATION: [e.g. Oval Office]

PARTICIPANTS: [Please refer to protocol list for correct order]

OUTLINE OF EVENTS: [Include description of the President's participation]

REMARKS REQUIRED: [To be provided by NSC][e.g. speech/keynote/brief]

MEDIA COVERAGE: [e.g. Open photo, writing pool, or WH Photographer]

FIRST LADY'S ATTENDANCE:

VICE PRESIDENT'S ATTENDANCE:

RECOMMENDED BY: [e.g. Department of State, NSC]

CONTACT: [Staff Member's Name & Ext]

ORIGIN OF THIS PROPOSAL: [e.g. Memorandum From...]

SECOND LADY'S ATTENDANCE:

CLASSIFICATION