

# Withdrawal/Redaction Sheet

## Clinton Library

| DOCUMENT NO.<br>AND TYPE | SUBJECT/TITLE                                                                                                                      | DATE                  | RESTRICTION                     |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------|-----------------------|---------------------------------|
| 001. memo                | <del>Samuel Berger et al. to the President re: Proposed Biological Terrorism Provisions in the Omnibus Crime Bill (12 pages)</del> | <del>05/13/1999</del> | <del>P5</del> <i>oms 4/6/15</i> |
| 002. paper               | re: President Clinton's Initiative on Biological and Chemical Weapons Preparedness (2 pages)                                       | 01/21/1999            | b(7)(E), b(7)(F)                |
| 003a. memo               | From: Samuel Berger re: Interview with Judy Miller and William Broad (5 pages)                                                     | 01/21/1999            | P1/b(1)                         |
| 003b. talking points     | re: Interview with Judy Miller and William Broad (2 pages)                                                                         | n.d.                  | P1/b(1)                         |

### COLLECTION:

Clinton Presidential Records  
Domestic Policy Council  
Devorah Adler  
OA/Box Number: 20146

### FOLDER TITLE:

Bioterrorism [Folder 4]

2012-0463-S

rc693

### RESTRICTION CODES

#### Presidential Records Act - [44 U.S.C. 2204(a)]

- P1 National Security Classified Information [(a)(1) of the PRA]
- P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
- P3 Release would violate a Federal statute [(a)(3) of the PRA]
- P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
- P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [(a)(5) of the PRA]
- P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

C. Closed in accordance with restrictions contained in donor's deed of gift.

PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).

RR. Document will be reviewed upon request.

#### Freedom of Information Act - [5 U.S.C. 552(b)]

- b(1) National security classified information [(b)(1) of the FOIA]
- b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
- b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
- b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
- b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
- b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
- b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
- b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

DEPARTMENT OF HEALTH AND HUMAN SERVICES  
THE GENERAL COUNSEL  
PHONE: 202/690-7741  
FAX: 202/690-7998

TO: DEVORAH ADLER / CHRIS JENNINGS

DATE: 5/14/99

DEPARTMENT/OFFICE: W.H./D.P.C.

PHONE: 456-5560

FAX: 456-5557

FROM: **HARRIET S. RABB**  
**GENERAL COUNSEL**

COMMENTS: Clear draft that went  
to WH Counsel  
and USE.

Cheers.

HSR

PAGES INCLUDING COVER: 13

XXXX

DRAFT-NOT FOR DISTRIBUTION

ACTION

## MEMORANDUM FOR THE PRESIDENT

THROUGH: THE EXECUTIVE CLERK

FROM: SAMUEL BERGER  
BRUCE REED  
NEAL LANE  
RON KLAIN  
JACK LEW  
CHARLES RUFF

SUBJECT: Proposed Biological Terrorism Provisions in the  
Omnibus Crime Bill

Purpose

To determine the Administration position on proposed biological terrorism provisions in the Omnibus Crime Bill.

Background

There is consensus within the Administration that serious gaps exist in current federal bioterrorism laws. In contrast to chemical, nuclear or radiological weapons, there are currently few laws in place designed to limit the availability of hazardous materials biological terrorists to the general public. While current laws are adequate to punish ~~perpetrators~~ after they unleash biological ~~agents~~ agents, they are not designed to ensure that these substances are kept out of the wrong hands in the first place. Additionally, bioterrorism is a growing concern in Congress and we believe that many on both sides of the aisle will be watching to see if the Administration will produce a draft bill with a strong law enforcement focus before introducing their own proposals.

[MOVE UP TO HERE TEXT ON P. 2]

DOJ's goal in proposing this legislation is to ensure that potentially hazardous biological materials do not fall into the wrong hands. HHS ~~does not disagree~~ with this goal, but is concerned that some of the proposed restrictions could chill vital scientific research into these agents that ~~may~~ be (will)

is in  
accord

may not achieve the desired goal and

cc: Vice President  
Chief of Staff

~~necessary to safeguard public health. With these dual concerns in mind~~ There is interagency agreement that the proposed Omnibus Crime Bill include new provisions establishing criminal penalties for:

- Possession of biological agents not justified by a peaceful purpose. Under this provision, whether possession is justified would be determined by type, quantity and purpose for possessing the agent.
- Unsafe handling of harmful biological agents. This provision would criminalize the actions of persons within the scientific community, but only to the extent that such persons handle harmful biological agents with conscious disregard for public health and safety in a manner that grossly deviates from accepted norms.
- Unregistered possession and unauthorized transfer of selected biological agents. This provision recognizes that authorities should be aware of who is handling the most deadly biological agents. Although establishing an initial inventory may pose a challenge to the scientific community, any additional reporting burden will be minimal for scientific facilities that already comply with CDC transfer regulations. You would have 60 days after this legislation takes effect to designate the agency that would be responsible for the registration process.
- Knowingly perpetrating a hoax regarding the use of biological agents. This provision is necessary given the recent spate of such hoaxes as the rash of anthrax scares around the United States.

~~In addition to these provisions,~~ The Administration will submit to Congress a statement indicating that we will review the bill's provisions with ~~representatives~~ representatives of the scientific community over a 60 day period, after which the Administration will advise Congress of any proposed changes deemed necessary.

~~necessary to safeguard public health and enhance national security.~~  
 Remaining Issues for Resolution

There is interagency disagreement on one remaining issue. Justice believes it is necessary to enact a provision which would, absent a waiver, criminalize the possession of dangerous ~~selected~~ agents by certain "restricted individuals". Justice believes that this provision, which permits waivers to be issued

MOVE UP TO PAGE 1 AS MARKED

(Set of) (Set of) [see Ridento p2]

Rider To Pz

In addition, HHS is ~~anxious~~ anxious not to incite intense opposition from the academic research, medical, scientific and public health communities that could jeopardize this initiative.

[return to "Remaining..." p2]

## QUESTION ON P3

The carry-over sentence on pp 2-3 says waivers are available "in most circumstances..." Two As later, the text says, "Under each category, waivers would be available."

---

Why the inconsistency?

RIDER TO P.3

"... needed to improve our counterterrorism capability both because the definition is too broad and, equally, because employers facing criminal liability for inappropriately granting waivers would be unlikely ever to use the option."

(Return to p 3)

## COMMENT ON THE RESTRICTIONS [PASSIM]

(A) Restricted persons would not pose a "safety" concern. They pose a security concern. Even hard-bitten spies are not particular safety risks in a lab due to poor techniques or reckless handling of select agents. We are concerned about them for reasons of security.

(B) Restricted persons are not disqualified from handling all biological materials, but rather only "select agents."

3

(See Addendum to p3)

in most circumstances, will be only minimally intrusive on the legitimate research community. NSC and DPC agree with DOJ.

HHS believes that the "restricted individual" provision as drafted would chill valid scientific endeavors. Thus HHS proposes a more narrow definition of "restricted individual". HHS believes that this narrower definition will sufficiently limit access to these dangerous agents while ~~protecting the privacy interests of the individuals involved and not unduly limiting scientific research.~~ HHS also proposes a different system for waivers. OMB, White House Counsel and OSTP agree with HHS.

*(one that would lessen the burden on employees and place the responsibility with the appropriate federal agency.)*

The different views with respect to the categories of individuals to be restricted are outlined below. Under each category, waivers would be available.

*needed to improve our counterterrorism capability.*

## 1. Individuals under indictment

DOJ believes that, absent a waiver, an individual under indictment for any felony should be restricted from handling biological agents because he or she may pose either a safety or security concern. HHS believes it is inappropriate to restrict an individual when the individual has yet to be convicted of any crime.

Option 1: Restrict access, absent a waiver, for any individual under indictment for any felony.

Option 2: Restrict access, absent a waiver, for any individual under indictment for any felony crime involving ~~the use or attempted use of force against another person or use of controlled substances where the maximum penalty is not less than five years, or bribery or espionage.~~

~~Option 3: Restrict access to individuals who are under indictment but have not been convicted of any crime.~~

## 2. Individuals convicted of a felony crime

DOJ believes that, absent a waiver, an individual who is convicted of any felony should be restricted from handling ~~biological~~ agents because they may pose ~~either a safety or~~ security concern. DOJ notes that such individuals lose many of their rights, including their right to vote. HHS believes that

PLEASE  
DO  
NOT  
LEAD  
WITH  
THIS;  
#2  
SHOULD  
COME  
FIRST

*moral turpitude*

*(select)*

*rationally related to the Nation's security interests sweeping in too broadly persons whose crime (e.g. vehicular homicide) is unrelated to security concerns.*  
 this provision is not ~~adequately tailored to catch those individuals who might pose a security risk or a danger.~~

Option 1: Restrict access, absent a waiver, for an individual convicted of any felony.

Option 2: Restrict access, absent a waiver, for any individual ~~under indictment for any felony crime involving the use or attempted use of force against another person or use of controlled substances~~ where the maximum penalty is not less than five years, ~~or bribery or espionage.~~

*(convicted)*

*moral turpitude*

*Editorial Note: Since this is not in dispute, should it be listed here?*

3. Individuals who are fugitives from Justice

Everyone concurs that this provision should be included.

4. Individuals who are unlawful users or are addicted to any controlled substance

DOJ believes that individuals who are either addicted to or users of controlled substances should be restricted from handling biological agents because they may pose either a safety or security concern. HHS believes that this provision is not adequately tailored to catch those individuals who might pose a security risk or a danger.

Option 1: Restrict individuals are using or are addicted to any controlled substance.

Option 2: Do not restrict such individuals.

5. Individuals who have been adjudicated as mental defective or committed to a mental institution

DOJ believes that an individual who has been adjudicated as a mental defective or who has been committed to a mental institution could pose a security ~~threat~~. HHS believes it is inappropriate to ~~inquire into the mental history of the individuals involved.~~ Mrs. Gore, as mental health advisor strongly agrees with the HHS position.

*exclude a scientist for a mental illness the treatment of which included hospitalization.*

Option 1: Restrict individuals who have been adjudicated as mentally defective or have been committed to any mental institution,

*SEE RIDER TO P.4*

RIDER TO P4**4. Individuals who are unlawful users of or are addicted to any controlled substance.**

(who are)  
DOJ believes that individuals who are either addicted to or unlawful users of controlled substances should be restricted from handling select agents because they may pose a security concern. HHS does not object to a restriction on unlawful users of controlled substances, but believes that a restriction on individuals addicted to (or in other words, dependent on) legally obtained controlled substances (for example, medication for chronic pain used under a physician's prescription) is not rationally related to the determination whether an individual is a security risk and would in any case be unadministrable.

- \_\_\_\_\_ Option 1: Restrict individuals who are unlawfully using or are addicted to any controlled substance.
- \_\_\_\_\_ Option 2: Restrict individuals who are unlawfully using any controlled substance.

5

Option 2: Do not ~~restrict such individuals.~~ *adopt this overbroad restriction.*

6. Alien other than an alien lawfully admitted for permanent residence *[SEE RIDER TO P. 5]*

Option 1: Restrict access of all non-permanent residents.

Option 2: Restrict access of only persons who are citizens of countries designated by the Secretary of State as sponsors of terrorism.

Option 3: Restrict access of non-permanent resident aliens who are citizens from countries other than NATO and major non-NATO allies (as defined in the Foreign Assistance Act).

7. Dishonorably discharged from the Armed Forces

DOJ believes that an individual dishonorably discharged for any reason should be restricted from handling ~~biological~~ *(select)* agents absent a waiver because he or she may pose ~~either a security concern.~~ HHS believes that only ~~certain categories of these persons dishonorably discharged should be restricted, i.e., those who have been dishonorably discharged for a reason similar to the felony category outlined above~~ *should be restricted.*

Option 1: Restrict access for an individual dishonorably discharged for any reason.

Option 2: Restrict access for any individual dishonorably discharged for ~~any~~ *moral turpitude* felony crime involving ~~the use or attempted use of force against another person or use of controlled substances~~ where the maximum penalty is not less than five years, ~~barbary or espionage.~~

8. Responsibility for Waiver Determinations

There is ~~also~~ disagreement over how the waiver provisions should be handled. The Justice provision allows availability of waivers where disabling criteria are not ongoing. For example, in cases where the disqualifying event is more than five years old and the employer makes a written determination that the employee is suitable or if the employee is a lawful, non-permanent resident alien and receives an immediate waiver from an agency designated by you. HHS agrees that waivers should be available, but believes that DOJ, not the employer, should be responsible for granting waivers. ~~to ease employer~~

## RIDER To P. 5

Insert DOJ Rationale + then continue introductory text as follows:

" AHS is concerned that the DOJ restriction sweeps too broadly. American biomedical research is deeply intertwined with opportunities for international collaborative research involving foreign students and scientists in training and research in our laboratories."

### [New Option]

" Option # : Designating non-access

aliens beyond those in Option 2

should be carefully and better done

after consultation with the scientific community."

~~Concerns about incurring liability as a result of issuing a waiver.~~

Concur with HHS Option on waivers \_\_\_\_\_

Concur with DOJ Option on waivers \_\_\_\_\_

DRAFT- NOT FOR DISTRIBUTION

Putting the burden of waivers on an employer whose decisions subject him or her to criminal penalties can be expected to cause employers to simply conclude that the risks and burdens were unacceptable, leading to rejection of the scientist or abandonment altogether of select agent research. Moreover there is no basis to believe that scientific employers have the expertise to assess national security risk.

- Option 1: Place the responsibility for waiver decisions, enforced by criminal penalties, on the employer.
- Option 2: Place the waiver responsibility in the Department of Justice.
- Option 3: Place the waiver responsibility in another federal agency qualified to make national security waiver decisions.

# ISSUE BRIEF

NATIONAL  
HEALTH  
POLICY  
FORUM

## Biological Terrorism: Is the Health Care Community Prepared?

Thursday, February 11, 1999

8:30 to 9:00 am - Continental Breakfast

9:00 am to noon - Discussion

210 Cannon House Office Building

A roundtable discussion with

**Margaret A. Hamburg, M.D.**

*Assistant Secretary for Planning  
and Evaluation*  
Department of Health and  
Human Services

**Scott R. Lillibridge, M.D.**

*Director, Bioterrorism Preparedness  
and Response*  
National Center for Infectious  
Diseases  
Centers for Disease Control and  
Prevention

**Donald A. Henderson, M.D., M.P.H.**

*Director*  
Center for Civilian Biodefense Studies  
School of Hygiene and Public Health  
Johns Hopkins University

**Davi M. D'Agostino**

*Assistant Director*  
National Security and International  
Affairs Division  
General Accounting Office

**Jerome M. Hauer**

*Director*  
Mayor's Office of Emergency  
Management  
New York

**Robert F. Knouss, M.D.**

*Director*  
Office of Emergency Preparedness  
Department of Health and  
Human Services

**Peter Rosen, M.D.**

*Professor of Clinical Medicine and  
Surgery*  
University of California, San Diego

**Robert M. Blitzer**

*Associate Director*  
Center for Counterterrorism,  
Technology, and Analysis  
Science Applications International  
Corporation  
McLean, Virginia

Registration: Please call **Dagny Wolf** at 202/872-1392 as soon as possible.

The  
George  
Washington  
University  
WASHINGTON DC

## Biological Terrorism

The nature of terrorism is changing. It is no longer only hijackers and bombs. Nor is it only chemical attacks, such as the 1995 Aum Shinrikyo Sarin gas attack in the Tokyo subway. With recent events in Iraq and elsewhere making headlines, biological agents have joined more traditional methods in the public awareness. Similar to chemical terrorism in some ways, bioterrorism differs primarily in the lag time between the terrorist event and its medical consequences. It therefore poses its own critical challenges, particularly for the public health community. Chief among these is assessing just how great a threat is posed by particular agents and improving the nation's surveillance and response capabilities.

To assist in assessing the risk, the Senate Veterans Affairs Committee and other committees have asked the General Accounting Office (GAO) to gather information on the "science behind the threat."<sup>1</sup> Defining the threat is particularly problematic and raises many questions: How available are biological agents? How easy would it be for terrorists to "weaponize" and use them? Are biological agents becoming the weapons of choice for terrorists? Given limited dollars, how and where and on which specific agents should preparedness experts focus their efforts and resources? While some experts disagree about the precise probability of a specific bioterrorist event, others stress that even low-probability events with high-consequence outcomes demand careful attention and planning. Even accidental exposures to biological agents and hoaxes, such as the recent California anthrax pranks, have critical implications for preparedness.

Successful preparation will depend upon the development of a well-orchestrated plan to be used by the civilian personnel first responding to an event. First responders will vary, depending upon the nature of the attack. For biological terrorism, they will be epidemiologists, infectious disease experts, emergency room personnel, and critical care unit personnel. These are the persons who are most likely to discover and need to respond initially to acts of bioterrorism because serious attacks with bioweapons would presumably cause epidemics. The traditional first responder community for chemical or explosive events—fire, police, hazardous materials (HAZMAT) teams, and emergency medical technicians—would be complementary but not central to the management of an epidemic caused by bioweapons.

Given the extreme importance attached to the readiness of civilian medical first responders and the growing appreciation for the likelihood of a biological terrorist event to occur in the United States, the U.S. Department of Health and Human Services' Office of Emergency Preparedness (OEP) asked the Institute of Medicine (IOM) in conjunction with the National Academy of Sciences' Commission on Life Sciences to:

- Collect and assess existing research, development, and technology information on detecting potential chemical and biological agents and protecting and treating both the targets of attack and health care providers.
- Provide specific recommendations for priority research and development.

The IOM report, *Chemical and Biological Terrorism: Research and Development to Improve Civilian Medical Response*,

identifies more than 60 research and development projects potentially useful in minimizing damage caused by a terrorist attack, including new drugs and vaccines, faster and easier-to-use chemical detectors and diagnostic tests, and communications software to improve disease surveillance and provide information about possible attacks. The report also discusses steps that could be taken to improve the capabilities of public health departments, poison control centers and metropolitan police departments.

(See Table 1-1 at the end of the issue brief.)

### ISSUE BRIEF/No. 731

**Analyst/Writer**  
Robin Strongin

**National Health Policy Forum**  
2021 K Street, NW, Suite 800  
Washington, DC 20052  
202/872-1390  
202/862-9837 (fax)  
nhpf@gwu.edu (e-mail)  
www.nhpf.org (Web site)

**Judith Miller Jones**, Director  
**Karen Matherlee**, Co-Director  
**Sandra M. Foote**, Co-Director  
**Michele Black**, Publications Director

**NHPF** is a nonpartisan education and information exchange for federal health policymakers.

This Forum session will use the IOM's study as a springboard for understanding the role the health care community must play in the event of a domestic biological terrorist attack. Speakers—focusing primarily on bioterrorism, as opposed to chemical<sup>2</sup> or radiological terrorism—will highlight the issue of threat assessment and discuss ways to improve the current level of preparedness as well as steps needed to convert the public health system into our best form of civil defense.

## BIOLOGICAL WARFARE 101

The use of microorganisms and toxins as weapons of destruction has a long history, with examples of biological terrorism dating back to before the 14<sup>th</sup> century. Methods used have ranged from deliberately infecting water supplies with diseased cadavers to passing out smallpox-infected blankets to "extirpate" Native American tribes in 1763.<sup>3</sup> Other examples include the use of fomites (objects that harbor and can transmit disease agents), as the Viet Cong did in the early 1960s when they smeared pungent sticks with excrement.<sup>4</sup>

Diseases resulting from biological agents, whether spread person-to-person or through other means, have incubation periods of days. This means, for example, that a person infected in a mass casualty attack could unwittingly continue to spread the disease, perhaps unleashing a deadly epidemic and most likely causing a wave of panic as the death toll mounted. Terrorists count on this added psychological dimension to erode trust in the target country's government and further cripple efforts at containment and control.

Biological agents considered to be priority biological terrorism threats can be categorized into three groups: *bacteria*, *viruses*, and *toxins*. In a March 8, 1998, *New York Times* article, Tom Kuntz excerpted the following from *Jane's Chem-Bio Handbook*, a "guide for military, police, and emergency personnel responding to suspected or real chemical or germ attacks."

**Anthrax.** Anthrax is an acute *bacterial* infection of the skin, lungs, or gastrointestinal tract. The skin infection can be caused by direct contact with contaminated wool, hides or [livestock] tissues. . . . As a biological weapon, it is expected that anthrax spores would be released at a strategic location to be inhaled. Inhalation anthrax results from deposition of the bacterial spores in the lungs and causes fever, shock, and eventually death. . . . Iraqi and Soviet biological warfare programs worked to develop an anthrax weapon.

**Ricin.** Ricin is a *toxin* made from the mash left over after processing castor beans for oil. Castor bean processing is a worldwide activity; therefore, the raw

materials for making ricin are easily available. Ricin is easy to produce and is stable. Ricin was used in 1978 by Bulgarian intelligence operatives in the "umbrella murder" of Gregori Markov, a Bulgarian dissident. A ricin-tipped bullet was discharged into the victim, and he died a day after the attack.

**Ebola.** Ebola *virus* is one of the most pathogenic viruses known to science, causing death in 50 to 90 percent of all clinically ill cases. . . . The Ebola virus is transmitted through direct contact with the blood, secretions, organs, or semen of infected persons. Transmission of the virus has also occurred by handling ill or infected chimpanzees. The virus has an incubation period of 2 to 21 days, and is characterized by sudden onset of fever, weakness, muscle pain, headache and sore throat. This is followed by vomiting, diarrhea, rash, limited kidney and liver functions and both internal and external bleeding. . . . Ebola viruses must be considered to have a high priority as a candidate for biological warfare. . . . This virus was assigned high priority in the former offensive program of the Soviet Union.

Additional biologic agents potentially available to bioterrorists include smallpox, brucellosis, plague, Q fever, tularemia, viral encephalitides, viral hemorrhagic fevers, botulinum, and staphylococcal enterotoxin B.

## DETECTING BIOLOGIC AGENTS: THE ROLE OF THE CDC AND STATE HEALTH DEPARTMENTS

Detecting and isolating biologic agents requires not only the ability of clinicians to identify and accurately diagnose uncommon diseases but also a surveillance system for collecting reports of such cases. Fortunately, the Centers for Disease Control and Prevention (CDC) operate a large number of infectious disease surveillance systems based on voluntary collaboration with state and local health departments, surveys, vital records, or registries. Unfortunately, the IOM report noted:

The best known of these systems, the National Notifiable Disease Surveillance System, currently includes several, but not all, of the diseases considered likely to be used in bioterrorism, and, like all passive surveillance systems, suffers from omissions and long-delayed reports. All of the systems depend upon confirmed diagnosis and are thus no help to a puzzled physician trying to arrive at a diagnosis. No federal funds are provided to state and local health departments to support these systems, and states' ability or willingness to support infectious disease surveillance has declined in recent years. CDC's Emerging Infections Program (EIP) is attempting to reverse this trend by making grants to state and local health departments

for improving epidemiological and laboratory capability. Expanding the activities of these centers would be an excellent way to raise both the awareness of bioterrorism and the ability to respond to it.

### **Bioterrorism: A Possible Scenario**

In his testimony on June 2, 1998, before the Senate Committee on Labor, Health and Human Services, and Education's Subcommittee on Appropriations, Edward Thompson, M.D., the health commissioner for the State of Mississippi, explained:

The likely scenario that a few major cities have either already tested, or are planning to test, in a table top exercise unfolds as follows: A bioterrorist event occurs involving the unannounced release of anthrax spores in an open air location during a major public event. The first responsibility immediately falls to the local health department to detect that an unusual number and type of case reporting is occurring. Responsibility for diagnosis of the agent falls next to the local or state public health laboratory. Investigation, by interviewing victims, again is the responsibility of the local health department, with assistance from the state health department, in order to identify the source of the agent, when the release took place, and who might have been exposed. Other critical phases of the exercise where major responsibility falls to the local health department, with assistance from the state health department, involves the distribution of vaccine and other essential treatment resources and distribution of diseased victims around the state and region as thousands become symptomatic.

In his testimony, Thompson stated,

Essential state health department functions in preparing for and responding to a bioterrorist incident would involve the following activities: epidemiologic surveillance, laboratory analysis, epidemiologic investigation, information and communications systems, and coordination of essential equipment and treatment (including health care facilities and personnel, isolation beds, and the availability and distribution of vaccines and other necessary treatment resources).

Experts all agree that states are ill-prepared to respond to a bioterrorist event. To underscore the current lack of preparedness among state health departments, Thompson quoted from a draft document on catastrophic disaster and terrorism by the Illinois Department of Health:

The Department is mandated to protect the public health and safety of the citizens of Illinois. However, limited opportunities have been made available to adequately prepare staff for a response to a terrorist incident involving radiological, biological, or chemical materials. Therefore, the Department's response

capabilities are currently limited. Several factors have prevented the Department from attaining a higher level of preparedness. These factors include: absence of a consistent funding source for training and education programs; limited personnel in infectious diseases, environmental health and laboratory services programs; and a lack of Federal guidance and information on source standards and detection methods.

Local and state health departments cannot fight terrorism alone. Emergency medical personnel as well as hospital personnel will also play a vital role in responding to biological and chemical incidents and reducing their consequences. In an effort to improve the preparedness of medical civilian responders, Congress in 1996 established the Domestic Preparedness Program, or DPP, under the Department of Defense. DPP, also referred to as the Nunn-Luger-Domenici program, appropriated funds to help train local first responders. Estimates indicate that approximately \$92 million has been appropriated in fiscal years 1997 and 1998 to enable the U.S. Army to deliver special "train the trainer" tutoring programs, to conduct exercises to test what has been learned, and to assist in the creation of medical strike teams in some of the largest American cities.

### **CRISIS AND CONSEQUENCE: MANAGING TERRORIST ATTACKS**

According to the September 1997 GAO report *Combating Terrorism: Federal Agencies' Efforts to Implement National Policy and Strategy*:

U.S. policy on combating terrorism has been evolving for about 25 years. In June 1995, the President issued Presidential Decision Directive 39 (PDD 39), "United States Policy on Counterterrorism," the central blueprint for the U.S. counterterrorism strategy. PDD 39 restated standing U.S. policy and elaborated a strategy for combating terrorism and measures to implement it. The U.S. strategy consists of three main elements: (1) reduce vulnerabilities and prevent and deter terrorist acts before they occur; (2) respond to terrorist acts that do occur, including managing crises and apprehending and punishing terrorist perpetrators; and (3) manage the consequences of terrorist attacks.

More recently, in May 1998, PDD 62 ("Combating Terrorism") and PDD 63 ("Critical Infrastructure Protection") were both issued. These directives establish a national coordinator for security, infrastructure protection, and counterterrorism and authorize the Federal Bureau of Investigation (FBI) to set up a National Infrastructure Protection Center to issue warnings to public and private operators of essential elements of the U.S. government and economy. In addition, the directives include a four-

part initiative focused on biological weapons. According to the IOM report,

It calls for a national surveillance system based on the public health system, provision of local authorities with necessary equipment and training, stockpiles of vaccines and specialized medicines, and a research and development program on pathogen gene mapping to guide development of new and better medicines and vaccines.

Preparing to meet the needs of civilian victims of a bioterrorist attack will require the coordination of the health care community as a whole, as well as of many other organizations, experts, and agencies at all levels of government. It has been estimated that more than 40 federal departments, agencies, and bureaus have some role in combating terrorism. Part of the challenge, not surprisingly, involves working through the complex maze of multiple bureaucracies to figure out who does what when and who reports to whom.

Generally, if an incident occurs without a warning, crisis and consequence management will be concurrent. The FBI would be in charge of crisis management (that is, controlling the crime scene and gathering evidence used to prosecute the terrorists). Primary responsibility for consequence management, however, rests with the states. The federal government supports state and local governments in domestic incidents through the Robert T. Stafford Disaster Relief and Emergency Assistance Act. The Federal Emergency Management Agency coordinates the federal response through a generic disaster contingency plan known as the Federal Response Plan, which categorizes types of federal assistance into specific emergency support functions. Support functions include, for example, health and medical services, urban search and rescue, and information and planning.

## Policy Dilemmas

In addition to organizational and chain-of-command issues, other policy quagmires need to be sorted out. For example, as Sean Paige wrote in his January 26, 1998, *Insight* cover story, "At the Eleventh Hour,"

Often the government seems to be working at cross-purposes—certain pieces of lifesaving protective gear much in demand by first responders across the country are off-limits to them because they don't meet workplace-safety standards. Yet these same items often are widely used by the military or approved for use in foreign countries.

The IOM draft report noted a similar dilemma.

With a few exceptions, treatment of a very small number of individuals exposed to any chemical or

biological agent is not beyond current medical capabilities. However, large numbers of casualties will quickly overtax those capabilities. Vaccines, drugs, antitoxins, and supportive medical equipment are generally available in small quantities. Moreover, many of the vaccines and antitoxins are not FDA [Food and Drug Administration] approved and are only available as Investigational New Drugs (INDs). This means not only that the product is only available in limited amounts, but that it can be used only in a research setting with the informed consent of the recipient. Thus, IND status effectively precludes use in a mass-casualty situation.

The final IOM report added the following:

FDA recognized the difficulty IND status presented in potential mass-casualty situations during the Persian Gulf War and passed an interim rule waiving the requirement for the United States military to obtain informed consent in using two investigational products intended to provide protection against chemical and biological warfare agents. The FDA has recently solicited comments on the wisdom of revoking this interim rule as well as on the nature of the evidence that ought to be required when products cannot ethically be tested in humans.

## PAYING FOR PREPAREDNESS

Increasing the level of preparedness is not cheap. In addition to funds appropriated more generally to counterterrorism efforts, Congress appropriated funds for bioterrorism and related public health infrastructure activities within DHHS. Specifically, the *Omnibus Consolidated and Emergency Supplemental Appropriations for FY99* allocated \$216,922,000 to the Public Health and Social Services Emergency Fund. According to the conference report, "The fund addresses the Administration request for bioterrorism and related activities as well as for bolstering public health infrastructure, conducting studies regarding health and national security, and combating certain infectious diseases."

According to the conference report, the \$216,922,000 is to be allocated as follows:

- \$154,750,000 for the CDC for a variety of activities. These include: \$1 million for the development of an overall preparedness plan, \$1 million to enhance technical capabilities to identify certain biological agents, \$51 million<sup>5</sup> for the CDC to establish a pharmaceutical and vaccine stockpile for civilian populations,<sup>6</sup> \$1.75 million for conducting independent studies of health and bioterrorism threats specified in the Senate report, \$2 million to assist states in developing emergency preparedness and

response plans, \$2 million to expand the CDC Epidemic Intelligence Service, \$2 million for regional laboratories for measuring chemical exposures, \$5 million to better identify potential biological and chemical terrorism agents, \$5 million to develop new sources and methods for surveillance, \$5 million to develop rapid toxic screening, \$5 million for the environmental health laboratory, \$7 million to strengthen state and local epidemiological and surveillance capacity, \$11 million for regional laboratories for detecting and measuring biological and chemical agents, \$28 million to establish a national health alert network, \$20 million for polio eradication activities, and \$8 million for measles eradication activities.

- \$12,172,000 for the Office of the Secretary, allocated as follows: \$2.5 million for the Office of Emergency Preparedness for a national disaster medical system, \$1.5 million for developing national response capabilities, \$3 million for metropolitan medical response systems, \$1.85 million for a nuclear weapons radiation study, and \$3 million in for the renovation and modernization of Fort McClellan's Noble Army Hospital in Alabama for bioterrorism training activities. The conference agreement also included \$322,000 to be provided to Calhoun County, Michigan, for reimbursement of certain expenses related to food-borne illnesses.
- The remaining approximately \$50 million is to be used "to address the HIV/AIDS crisis facing the African American community and other racial and ethnic minority communities due to the changing demographics of the disease."

## THE FORUM SESSION

The Forum has invited a number of experts to help sort through how the health care community can better prepare for and contribute to the prevention of a biological terrorist attack. **Margaret A. Hamburg, M.D.**, assistant secretary for planning and evaluation within DHHS and a past commissioner of health for the City of New York, will set the stage by addressing the following: What are we preparing for? How well prepared are we? And what do we need to do in the short-term and the long-term? Dr. Hamburg has a distinguished record of scientific accomplishments and outstanding public service. She has been elected to membership in the Institute of Medicine, the New York Academy of Medicine, and the Council on Foreign Relations and is a fellow of the American Association of the Advancement of Science.

Following Dr. Hamburg's remarks panelists representing several areas of expertise will participate in a roundtable discussion focusing on the following questions:

- What are the medical and public health ramifications of a bioterrorist event?
- What are the most serious bioweapons facing the public health community today?
- How prepared or ill-prepared are various sectors of the health community to respond to a successful bioterrorist attack of any proportion?
- What kind of practical steps could be taken to reduce the risk? To minimize the consequences?
- How much would such steps cost? How should they be funded?
- What are the research needs? Who should be conducting the research?
- What are the commonalities and differences between chemical and biological terrorism? What elements need to be considered in preparedness planning and resource allocation? Should biological and chemical terrorism be linked or unlinked for planning purposes?

**Scott R. Lillibridge, M.D.**, director of the CDC's bioterrorism preparedness and response activities, was the lead public physician during the initial U.S. Public Health Service response to the Oklahoma City bombing and was team leader for the U.S. Medical Delegation to Tokyo following the Sarin release in 1995.

**Davi M. D'Agostino**, assistant director of GAO's National Security and International Affairs Division, has been leading GAO's work on crosscutting counterterrorism issues for the past three years. In 1995, Ms. D'Agostino was selected to attend the Industrial College of the Armed Forces. She received the GAO Meritorious Service Award in 1997.

**Robert F. Knouss, M.D.**, director of the DHHS Office of Emergency Preparedness, also directed the Public Health Service's refugee health activities during the Cuban-Haitian entrant and Southeast Asian refugee crisis and served as deputy director of the Pan American Health Organization.

**Peter Rosen, M.D.**, director of the emergency medicine residency program at the University of California, San Diego and professor of clinical medicine and surgery there, also served as chair of the IOM's January 1999 study, *Chemical and Biological Terrorism: Research and Development to Improve Civilian Medical Response*.

**Donald A. Henderson, M.D., M.P.H.**, director of the Johns Hopkins Center for Civilian Biodefense Studies, is also the Johns Hopkins University Distinguished Service Professor and has appointments in the Departments of Epidemiology and International Health in the School of Hygiene and Public Health. Dr. Henderson also served as dean of the faculty of the Johns Hopkins School of Public Health and directed the World Health Organization's global smallpox eradication campaign.

**Jerome M. Hauer**, director, New York City's Office of Emergency Management, served on the faculty of the Northeastern University Paramedic Program, joined the Biomedical Division of IBM as clinical research coordinator, and served as a volunteer firefighter and as a member of a HAZMAT team in Connecticut. Mr. Hauer is a member of the New York City Police Department's Honor Legion.

**Robert M. Blitzer**, associate director of the Center for Counterterrorism, Technology, and Analysis at Science Applications International Corporation, recently retired from the Federal Bureau of Investigation, where he served as the chief of the bureau's domestic terrorism section.

---

## ENDNOTES

1. The GAO report, due this summer, will be classified. The unclassified version will be available this fall.
2. Includes nerve agents such as Sarin, blister agents such as mustard and Lewisite, and pulmonary agents such as pulmonary phosgene.
3. E. Wagner Stearn and Allen E. Stearn, *The Effects of Smallpox on the Destiny of the American Indian* (Boston: Bruce Humphries, 1945), 44-5.
4. G. W. Christopher et al., "Biological Warfare: A Historical Perspective," *Journal of the American Medical Association*, 278 (August 6, 1997), no. 5: 412.
5. This money cannot be obligated until DHHS submits an operating plan to both the House and Senate Appropriations Committees.
6. The House bill provided for this activity at CDC as non-emergency funding while the Senate bill provided for this activity at the Office of Emergency Preparedness. Additionally, the conference agreement "assumes that within the overall increase provided for NIH, \$10,000,000 will be allocated for vaccine research and development activities in support of the bioterrorism initiative."

**Table 1-1: Relative Capabilities for Response to Civilian Chemical and Biological Incidents at Four Levels of Medical Care**

| Capability                                                                 | Local Responders |            | Initial Treatment Facilities |            | State    |            | Federal  |            |
|----------------------------------------------------------------------------|------------------|------------|------------------------------|------------|----------|------------|----------|------------|
|                                                                            | Chemical         | Biological | Chemical                     | Biological | Chemical | Biological | Chemical | Biological |
| Receipt of pre-incident intelligence                                       | L                | L          | L                            | L          | S        | S          | S        | S          |
| Detection, identification, and quantification of agents in the environment | S                | L          | L                            | L          | S        | S          | H        | S          |
| Personal protective equipment                                              | S                | S          | L                            | S          | L        | S          | S        | S          |
| Safe and effective patient extraction                                      | S                | S          | N/A                          | N/A        | N/A      | N/A        | S        | S          |
| Methods for recognizing symptoms and signs in patients                     | S                | S          | S                            | S          | L        | L          | S        | S          |
| Detection and measurement of agent exposure in clinical samples            | L                | L          | L                            | S          | L        | S          | H        | H          |
| Methods for recognizing covert exposure in populations                     | N/A              | N/A        | S                            | S          | S        | S          | S        | S          |
| Mass-casualty triage techniques and procedures                             | S                | S          | S                            | S          | L        | L          | S        | S          |
| Methods/procedures for decontamination of exposed individuals              | S                | S          | L                            | L          | L        | L          | S        | S          |
| Availability, safety, and efficacy of drugs and other therapies            | L                | L          | S                            | S          | L        | L          | S        | S          |
| Prevention, assessment, and treatment of psychological effects             | S                | S          | S                            | S          | S        | S          | S        | S          |

NOTE: H = highly capable; S = some capability; L = little or no capability; and N/A = not applicable.

Source: Institute of Medicine, *Chemical and Biological Terrorism: Research and Development to Improve Civilian Medical Response* (Washington, D.C.: National Academy of Sciences, January 1999), 20.

Vdh -  
CDC

6/10/01

## Possible Non-Governmental Speakers

### Bioterrorism

1. **Dr. Joshua Lederberg**, Nobel Laureate and Sackler Foundation Scholar, Rockefeller University. Dr. Lederberg won the Nobel prize for Medicine for discovering genetic mechanisms in bacteria. He has long been a vocal international leader in the call for control of biologic weapons. **He was also a member of the President's roundtable on biological weapons last year.**
2. **Dr. Donald A. Henderson**, Director, Johns Hopkins Center for Civilian Biodefense Studies. From his previous position at the World Health Organization, Dr. Henderson led the international effort to eradicate smallpox.
3. **Dr. Michael Osterholm**, Chief, Acute Disease Epidemiology Section, Minnesota Department of Health. Dr. Osterholm is on the front lines of infectious disease surveillance and control, has published widely on the subject, and is an outspoken supporter of expanded national and local capacity to prepare for, and respond to, attacks of biological terrorism.
4. **Jerome M. Hauer**, Director, Office of Emergency Management, City of New York. New York has been at the forefront of preparedness for a terrorist attack involving weapons of mass destruction. Hauer has played a critical part in this effort, and has been vocal on this issue. He was also a member of the President's roundtable last year.

### Cyber Terrorism

1. **Norm Augustine**: Preferred. Just retired as CEO of Martin-Marietta. Professor at Princeton. A leading private sector spokesman on the cyber threat to critical infrastructure. Tentatively designated to head our National Infrastructure Assurance Council (CEOs of critical industries)
2. **Jamie Gorelick**: Currently at Fannie Mae. Former Deputy Attorney General. A co-chair of the Advisory Council to the President's Commission on Critical Infrastructure Protection.

Karin-

we need final budget #s on  
all these initiatives -

is this the right  
~~place~~ place to ask this?

**NATIONAL SECURITY COUNCIL****FAX COVER SHEET****NATIONAL  
SECURITY  
COUNCIL****17th & Penn, N.W.  
Washington, D.C.  
20504****Did you get a complete,  
clear transmission? If not,  
please call:****(202) 456-\_\_\_\_\_****From: Matt Gobush****To: Devorah Adler****Agency: DPC****Fax Number: 6-5557****Date/Time: 21 January****No. of pages to follow: 2****Message:****Please contact me at 69379 with any comments.  
Thanks.**

**FAX TRANSMITTAL SHEET****DATE:** 18 DECEMBER 1998

**TO:** DEVORAH ADLER  
**ORGANIZATION:** DOMESTIC POLICY COUNCIL  
**VOICE:** 202/456-5707  
**FAX:** 202/456-5557

**FROM:** BILL RAUB  
**ORGANIZATION:** DEPARTMENT OF HEALTH  
AND HUMAN SERVICES  
**VOICE:** 202/690-5874  
**FAX:** 202/205-8835  
**E-MAIL:** wraub@osaspe.dhhs.gov

**NUMBER OF PAGES FOLLOWING:** 5

**MESSAGE:** PER TELEPHONE CONVERSATION TODAY  
RE BIOTERRORISM

ACCOMPANYING THIS COVER SHEET ARE COPIES OF TWO ARTICLES THAT PROVIDE SOME CONTEXT. I HIGHLIGHTED ONE STATEMENT IN EACH THAT YOU MIGHT FIND HELPFUL.

I ADD ONLY THAT, IN CONSIDERING THE LIKELY SCOPE OF A BIOTERRORIST ATTACK, ONE NEEDS TO TAKE INTO ACCOUNT NOT ONLY THE VICTIMS BUT ALSO SEVERAL OTHER GROUPS: A) THOSE EXPOSED BUT NOT YET SYMPTOMATIC, B) THOSE POSSIBLY EXPOSED, AND C) THOSE NOT LIKELY TO HAVE BEEN EXPOSED BUT ANXIOUS THAT THEY WERE -- AKA, THE WORRIED WELL. PUBLIC HEALTH OFFICIALS WOULD BE REMISS WERE THEY NOT TO OFFER CHEMOPROPHYLLAXIS OR VACCINATION, WHERE AVAILABLE, TO INDIVIDUALS IN ALL THESE GROUPS. THUS, A RELEASE OF ANTHRAX IN NYC OR LA COULD REQUIRE THAT THE MEDICAL AND PUBLIC HEALTH RESPONSE DEAL WITH AS MANY AS 10 MILLION PEOPLE.

# Biological Terrorism

## Preparing to Meet the Threat

Jeffrey D. Simon, PhD

The threat of terrorists using biological warfare agents has received increased attention in recent years. Despite the hope that, with the right mix of policies, security measures, and intelligence gathering, a major biological warfare terrorist attack can be prevented, the history of conventional terrorism indicates otherwise. The greatest payoff in combating biological terrorism lies in focusing on how best to respond to a terrorist attack. The medical and emergency service communities will play the most important role in that process. Ensuring that they are trained to recognize the symptoms of diseases caused by biological warfare agents and have Critical Incident Stress Debriefing teams available to help them cope with the emotional aspects of treating exposed survivors should be part of contingency planning. By improving our readiness to respond to biological terrorism, many lives can be saved and terrorists denied their goal of creating panic and crisis throughout the country.

JAMA. 1997;278:438-439

THE THREAT of terrorists using biological warfare (BW) agents has received increased attention in recent years. Congressional hearings,<sup>1</sup> research studies,<sup>2,3</sup> government warnings,<sup>4</sup> and commentaries<sup>5,6</sup> have all pointed to a potentially more ominous terrorism future. Many factors account for this concern—revelations that Iraq, a state sponsor of terrorism, stockpiled anthrax, botulinum toxin, and other BW agents during the Persian Gulf War; the discovery that Aum Shinrikyo, the Japanese religious cult that released the chemical agent sarin in the Tokyo subway system in 1995, had a research and development program for BW agents; the low cost and minimum scientific knowledge required for producing BW agents; and the tendency for terrorists to move

into new areas of violence when current ones no longer achieve the intended effect—publicity, reaction, chaos.<sup>7</sup>

Despite this growing concern, however, we still know very little about the nature of BW terrorism. There has never been a major BW terrorist attack. Therefore, there is no track record of incidents, groups, tactics, motives, and targets for analysis to determine the best strategies for combatting this global threat. In this regard, we are today with respect to BW terrorism where we were nearly 30 years ago with respect to "conventional" terrorism. A new international threat was emerging then, but it was unclear as to the direction it would take.

It took several years after the first major international hijacking in 1968 for the diverse nature of conventional terrorism (hijackings, bombings, hostage situations) to become clear and for governments to take action against the threat. Biological warfare terrorism, however, will not allow governments, publics, and the international community the luxury of time to watch this

threat unfold and then determine the proper responses. Since BW terrorist attacks could have catastrophic effects in terms of lives lost and create a medical, political, and social crisis unparalleled in our history, it is important to prepare now for this new age of terrorism.

... we are today with respect to BW terrorism where we were nearly 30 years ago with respect to "conventional" terrorism.

The first step is to accept the reality that we will not be able to prevent every act of BW terrorism. Governments have learned that painful lesson with respect to conventional terrorism. While preventive measures must continue to be pursued, the greatest payoff in fighting BW terrorism lies in improving our response to an incident. There will be more opportunity for saving lives in the emergency medical response to a BW terrorist attack than in the response to a conventional terrorist attack. Whereas most of the fatalities in a conventional terrorist bombing occur immediately or shortly after the explosion,<sup>8</sup> in BW terrorism the incubation period for the virus, bacterium, or toxin could be several days. Accurate diagnosis and speedy treatment could save many lives.

The medical and health communities will therefore play the most significant role in combatting BW terrorism, and they will have to carry out their duties at a time of unprecedented crisis and fear throughout the country. To the extent that we can reduce the uncertainty about how BW terrorist incidents are likely to

From the Office of the President, Political Risk Assessment Co, Inc (a consulting firm in security and terrorism research), Santa Monica, Calif.

Dr Simon has received royalties for his book, *The Terrorist Trap: America's Experience With Terrorism* (Indiana University Press, 1994).

Reprints: Jeffrey D. Simon, PhD, Political Risk Assessment Co, Inc, PO Box 82, Santa Monica, CA 90406 (e-mail: jdaimon@earthlink.net).

unfold, the better the medical and health professions will be prepared to deal with the aftermath of this most dangerous form of global terrorism.

## BIOLOGICAL TERRORISM: LIKELY TACTICS AND TARGETS

The most distinguishing feature separating BW terrorism from conventional terrorism is the extraordinarily larger number of casualties that could follow a major terrorist attack involving biological agents. Whereas bombings of airplanes or buildings with conventional explosives have occasionally resulted in a few hundred deaths, each act of BW terrorism could result in hundreds of thousands or even millions of casualties.<sup>2</sup> Adding to the death toll would be the fact that civilian populations are not immunized against most BW agents and do not have protective equipment, such as filtered respirators and gas masks, readily available.<sup>1</sup>

Some biological agents have been used in the past for selective attacks. For example, Bulgarian agents assassinated Georgi Markov, a Bulgarian émigré and writer for the British Broadcasting Company, by stabbing him in London with an umbrella-type weapon that contained ricin,<sup>11</sup> which is a potent protein toxin derived from the bean of the castor plant (*Ricinus communis*).<sup>12</sup> (Another Bulgarian émigré, Vladimir Kostov, was attacked in a similar fashion in Paris in 1978, but lived when physicians removed the pellet containing ricin from his body.) However, a terrorist group that uses BW agents will likely be attracted to the mass killing potential of these weapons. It makes little sense for terrorists to experiment with dangerous biological agents—they could be killed handling and using them—if their goal is a limited attack that could have been achieved by using safer and more familiar conventional weapons.

Biological warfare terrorism will also encompass a narrower range of tactics than conventional terrorism. Although BW agents could be used during a hijacking or hostage situation, there would be little incentive for terrorists to do so. The projected death toll would be no higher than if conventional weapons were used. And while BW agents could be delivered against a target by means of a bomb or missile, the likelihood that the organisms will be destroyed in the explosion makes this an unattractive delivery method.<sup>2</sup>

Rather, the most likely BW terrorist tactic will be to release BW agents—anthrax spores, botulinum toxin, ricin, or other deadly agents—into the air as a biological aerosol, a stable cloud of suspended microscopic droplets of bacterial or virus particles.<sup>3</sup> Since BW agents are invisible, odorless, and tasteless, no one would know that a terrorist attack is under way.

The aerosol of BW could be accomplished in several ways, including using low-flying airplanes, crop dusters, or trucks equipped with spray tanks and releasing the BW agent upwind of populated areas; leaving aerosol canisters filled with the BW agent and timing devices in subways, airports, air-conditioning/heating systems in buildings, or other crowded places; or directly contaminating bulk food supplies in restaurants, supermarkets, or other places with a BW agent. However, large US water supplies such as a city water supply would not be an attractive target for contamination due to the large amount of BW agent required and water purification procedures used by most cities in the United States.

Since there are no reliable detection systems for BW agents, terrorists will be able to strike any target they desire. Whereas terrorists with conventional weapons have to be concerned about metal detectors, x-ray machines, and other physical security measures, terrorists with BW agents do not face those means of detection. With maximum casualties the likely goal, metropolitan areas are the most at risk. At the present time and for the foreseeable future, major cities in the United States and around the world remain indefensible to a BW terrorist attack.

## RESPONDING TO BW TERRORISM: UNCHARTERED WATERS

The heightened concern regarding biological terrorism has led to studies of how well prepared the United States is to respond to a major incident. The findings are not encouraging. During hearings held in 1995 and 1996, the US Senate Permanent Subcommittee on Investigations, for example, found that the United States did not have a plan that coordinated federal, state, and local agencies in managing the consequences of a terrorist attack with a weapon of mass destruction.<sup>1</sup> The subcommittee also found that principal field officers with police, fire, and emergency service departments in major cities are inadequately trained and do not have basic equipment to deal with biological, chemical, or nuclear terrorism, including protective gear, breathing apparatus, decontaminants, and antidotes.<sup>1,13</sup>

The lack of preparedness is attributable to several factors. One is that since the casualties from a biological terrorist incident are so disturbing even to think about, many public officials cling to the hope that with the right mix of police, security measures, and intelligence gathering, BW terrorism can be prevented. Funding for emergency responses to BW terrorism therefore has not been given the high priority it deserves until very recently. The second factor is the difficult task of plan-

ning for an event that has never occurred before. Emergency response teams are therefore left only with alternative scenarios to guide them in their plans.

An amendment to the 1997 Defense Authorization Act addresses some of these issues by calling for better training, equipment, and coordination among emergency response personnel in the United States to deal with a terrorist incident involving a weapon of mass destruction.<sup>14</sup> There is also a need for hospitals to have adequate supplies—or ways to quickly obtain these supplies—of antibiotics and antitoxins that could be used to treat those exposed to BW agents. Medical personnel also should be trained to recognize the different symptoms of various BW agents so that those exposed can be treated quickly. Most physicians do not see cases of anthrax in their daily practices.<sup>1</sup>

Since BW agents are invisible, odorless, and tasteless, no one would know that a terrorist attack is under way.

An important part of the response to BW terrorism will be dealing with the psychological reactions among survivors, emergency workers, and the public. Terrorism is a form of psychological warfare with terrorists often perpetrating their violence to cause fear among the public. In BW terrorism, that fear will understandably be great as people watch their fellow citizens fall ill and possibly die in large numbers due to anthrax, botulism, or other diseases. Contingency plans for dealing with public hysteria and disruption of health care delivery systems—including the possibility of health care professionals' becoming ill from the BW attack, or fleeing the affected area if they are not confident that they have adequate equipment to protect themselves—should be established in every large city.

The mental health of emergency workers and medical personnel will have to be monitored during a BW terrorism crisis. Research indicates that the most traumatic events for emergency nurses are the death of a child and the death of a coworker.<sup>15</sup> A major BW incident will likely have many of these types of victims. Dealing with dead bodies can also cause emotional and psychological problems for disaster rescue and recovery workers.<sup>6</sup> During a BW terrorist incident, rescue workers will face the unique situation of dealing with large numbers of deaths in a setting that otherwise seems very normal. There will not be any collapsed or bombed-out buildings, fires, plane crashes, and so forth. The psychological impact of that situation on first-

responders needs to be addressed in contingency plans.

The Critical Incident Stress Debriefing (CISD) process could help in dealing with the psychological aspects of a BW terrorist attack. This process is part of a broad crisis intervention program known as Critical Incident Stress Management (CISM), which is designed to prevent or mitigate the development of adverse psychological reactions among emergency service and public safety personnel, nurses, physicians, and disaster workers. The program has been used during earthquakes, plane crashes, terrorist bombings, and other tragic events. Through various psychological intervention techniques, a CISD team led by mental health professionals and including peer support personnel from the emergency services can help emergency workers and medical personnel recover as quickly as possible from the stress associated with the crisis.<sup>17</sup>

#### References

1. Global Proliferation of Weapons of Mass Destruction, Hearings Before the Permanent Subcommittee on Investigations of the Committee on Governmental Affairs, US Senate, 104th Cong, 1st Sess, Part 1, October 31 and November 1, 1995 (hearings also held by the Subcommittee on March 20, 22, and 27, 1996).
2. US Congress, Office of Technology Assessment. *Proliferation of Weapons of Mass Destruction: Assessing the Risks*. Washington, DC: Office of Technology Assessment; August 1993. Document OTA ISC 559.
3. US Congress, Office of Technology Assessment. *Technologies Underlying Weapons of Mass Destruction*. Washington, DC: Office of Technology Assessment; December 1993. Document OTA BP ISC 115.
4. Bailey KC. *Doomsday Weapons in the Hands of Many: The Arms Control Challenge of the 90s*. Urbana: University of Illinois Press; 1991.
5. Kupperman RH, Smith DM. Coping with biological terrorism. In: Roberts B, ed. *Biological Weapons: Weapons of the Future?* Washington, DC: Center for Strategic and International Studies; 1993:35-46.
6. G-7 [Group of Seven industrialized nations—United States, Japan, Germany, Britain, France, Italy, and Canada] Declaration on Terrorism. G-7 Economic Summit, Lyon, France, June 27, 1996.
7. Stephenson J. Confronting a biological Armageddon: experts tackle prospect of bioterrorism. *JAMA*. 1996;276:349-351.
8. Flanagan A, Lederberg J. The threat of biological weapons: prophylaxis and mitigation: call for papers. *JAMA*. 1996;276:419-430.
9. Simon JD. *The Terrorist Trap: America's Experiences With Terrorism*. Bloomington: Indiana University Press; 1994.
10. Mallonee S, Sharlat S, Stennies G, Waxweiler R, Hogan D, Jordan F. Physical injuries and fatalities resulting from the Oklahoma City bombing. *JAMA*. 1996;276:382-390.
11. Andrew C, Gordicovsky O. *KGB: The Inside Story*. New York, NY: HarperCollins; 1990:644-645.
12. US Army Medical Research Institute of Infectious Diseases. *Medical Management of Biological Casualties Handbook*. Ft Detrick, Frederick, Md: US Army Medical Research Institute of Infectious Diseases; August 1998:92.
13. Simon JD. The new age of terrorism. *Boston Globe*. April 19, 1996:19.
14. Sopko JF. The changing proliferation threat. *Foreign Policy*. 1996-1997;105:3-20.
15. Burns C, Harn NJ. Emergency nurses' perceptions of critical incidents and stress debriefing. *J Emerg Nurs*. 1998;19:431-436.
16. Skolnick AA. First complex disaster symposium features dramatically timely topics. *JAMA*. 1996;274:11-12.
17. Mitchell JT, Everly GS. *Critical Incident Stress Debriefing: An Operations Manual for the Prevention of Traumatic Stress Among Emergency Services and Disaster Workers*. 2nd ed rev. Ellicott City, Md: Chevron Publishing Corp; 1995, 1996.
18. Kahn H. *Thinking About the Unthinkable*. London, England: Weidenfeld & Nicolson; 1962.

#### CONCLUSION

Terrorists with BW agents pose a threat to this nation's—and all nations'—vital interests. In the 1960s, the physicist Herman Kahn wrote a book on fighting a nuclear war entitled *Thinking About the Unthinkable*.<sup>18</sup> Fortunately, we never had to experience that event, and the end of the cold war hopefully means we never will. But we face a new threat at the dawn of the 21st century, and it is one that we must think about and for which we must prepare. By improving our readiness to respond to a BW terrorist attack, many lives can be saved and the terrorists denied their goal of creating panic and crisis in this country.

I would like to thank Cornelius G. McWright, PhD, Douglas M. Snyder, PhD, Susan Snyder, MD, Laura J. Broadie, LCSW, BCD, and the 2 anonymous reviewers for their helpful comments on this article.

## Commentaries

# Why Should We Be Concerned About Biological Warfare?

There is a widespread tendency to think about defense against biological warfare as unnecessary, as someone else's responsibility, or as simply too difficult. Unfortunately, however, the dangers posed by biological weapons did not disappear when the United States began to unilaterally dismantle its own offensive program in 1969. The dangers did not vanish with the signing of the Biological and Toxin Weapons Convention of 1972, and they did not dissipate with the end of the Cold War or the threat of nuclear retaliation against Iraq during the Persian Gulf conflict. Only by planning and investing in the right training and defensive measures can we diminish the likelihood that biological weapons will be used and reduce the risks, disruption, and casualties in the event that such weapons are used.<sup>1</sup> Fortunately, significant improvements can be made in our defensive posture at relatively modest levels of investment, and both the Department of Defense and the medical community can play a substantial role in this regard.

Biological weapons are unfortunately characterized by low visibility, high potency, substantial accessibility, and relatively easy delivery. The basic facts are well known: a millionth of a gram of anthrax constitutes a lethal inhalation dose. A kilogram, depending on meteorological conditions and means of delivery, has the potential to kill hundreds of thousands of people in a metropolitan area. These small quantities make the concealment, transportation, and dissemination of biological agents relatively easy. Many of these agents—bacteria, viruses, and toxins—occur naturally in the environment. Moreover, many are used for wholly legitimate medical purposes (such as the development of antibiotics and vaccines), and much of the technology required to produce and “weaponize” them is available for civilian or military use. Unlike nuclear weapons, missiles or other advanced systems are not required for the delivery of biological weapons. Since aerosolization is the predominant method of dissemination, extraordinarily low-technology methods, including agricultural crop dusters, backpack sprayers, and even purse-size perfume atomizers will suffice. Small groups of people with modest finances and basic training in biology and engineering can develop an effective biological weapons capability. Recipes for making biological weapons are even available on the Internet.

These unique characteristics make both military and civilian society vulnerable to biological weapons. It is true that

their delayed effects and vulnerability to weather make these weapons ill-suited to military purposes such as seizing territory. But biological weapons can effectively impede the mobilization and massing of troops that would be required to sustain our role in a conventional conflict. Most disturbingly, they can be used to threaten civilian populations and create mass panic. Used this way, biological weapons can achieve military goals by undercutting the civilian support necessary for military operations or by holding civilians hostage to prevent military operations.

## Why Have Biological Weapons Been Low on Our Agenda?

If biological weapons are so potent and so cheap, if the technology is readily available, and if so many of our adversaries have biological warfare capabilities, then why has this issue been so low on our national security agenda?

There are 3 principal reasons. First, because defense against a biological attack is both unfamiliar and difficult, there is a natural tendency to put it aside in favor of problems that are more comfortable. This is abetted by a second factor: the belief that because biological weapons have never been used they therefore never will be. And this is in turn buttressed by a sense that a regime can be deterred from using biological weaponry if we make it clear that this would invite nuclear retaliation.

These modes of thought are dangerously inappropriate. If we address deterrence first, many argue that Saddam Hussein's unwillingness to unleash Iraq's biological arsenal, in the face of not-so-subtle threats of nuclear retaliation, validates the primacy of our deterrent. However, nations are not the only potential users of biological weapons. If one of the most likely scenarios entails their use by nonstate actors, small groups, or even individuals, a nuclear deterrent may be ineffective. Of course, terrorists can often be associated with state sponsors, but the quantum of proof we would require before responding to such a perceived linkage with a nuclear attack would be awfully high. Consider, for example, the forensic difficulty in assigning responsibility for the tragic attack against Pan Am Flight 103 that exploded over Lockerbie, Scotland, in 1988. In the event of a biological contingency, it is especially easy to mask the nature and source of an attack and even to obscure whether it is a natural occurrence. In such circumstances, can we credibly rely on a threat of assured nuclear retaliation? Depending on the agent used, if those exposed just got sick but did not die, what would constitute a proportional response?

The assumption that biological weapons will not be used in the future because they have not been used in the past is based on an error of fact. History is replete with examples in which biological weapons have been used, including the following: in the Middle Ages infected cadavers were catapulted over the walls of European cities and castles under siege; in

This commentary was written when both authors worked for the Office of the Undersecretary of the Navy, US Department of the Navy, Washington, DC. Mr. Danzig, a Washington, DC, lawyer, was undersecretary of the US Navy from November 1993 through May 1997. Ms. Berkowsky is now a special assistant in the Office of the US Secretary of Defense.

Reprints: Pamela B. Berkowsky, MALD, 1000 Navy Pentagon, Room 4E732, Washington, DC 20350-1000 (e-mail: berkowsky.pamela@osd.pentagon.mil).

the French and Indian Wars, the British supplied Indians with smallpox-infected blankets; during World War II, Japanese Unit 731 experimented with biological weapons on prisoners of war in Manchuria, resulting in more than 1000 deaths.

There are also abundant examples that bring the threat much closer to home. In 1995, 2 members of a Minnesota militia group were convicted of possession of ricin, which they had produced themselves for use in retaliation against local government officials.<sup>8,9</sup> In 1996, an Ohio man with connections to an extremist group was able to obtain bubonic plague cultures through the postal service.<sup>2</sup> It has even come to light that Aum Shinrikyo, the Japanese cult organization responsible for the sarin attacks on the Tokyo subway system, was working on anthrax and botulism as weapons.<sup>2</sup> The group's biological capability, its production and testing and laboratory infrastructure, and its experimental delivery systems existed for years while escaping detection by Western intelligence.

While it is often said that familiarity breeds contempt, no national security establishment can let unfamiliarity breed neglect. Biology is unfamiliar terrain. As Alan Beyerchen, PhD, has pointed out, the history of the absorption of technology into the war fighting capabilities of the Department of Defense suggests a reason for this blind spot.<sup>6</sup> World War I brought chemists and war fighters together; World War II brought physicists into the fold; and the cold war represented an era of the primacy of the computing, telecommunications, and electronics communities in the defense arena. What little connection the US government maintained with the biological community dissipated when, in 1969, we foreswore any offensive biological and toxin weapon capability. But our forbearance does not imply that of others. The United Nations' inspections of Iraq after the Persian Gulf conflict should be a wake-up call in this regard.<sup>7</sup> Along with the information of a high-level defector who had responsibility for Iraq's unconventional weapons program, these inspections revealed a large-scale biological production and "weaponization" effort that had gone substantially undetected by the West.

### What Should We Do About the Threat of Biological Warfare?

The Department of Defense has embarked on a challenging program to enhance its capabilities to defend against biological warfare. The program includes, among other things, the development and fielding of state-of-the-art biodetectors; the creation and designation of selected military units with expertise in medical prophylaxis, hazard mitigation, and decontamination; investments in vaccine and antibiotic research, development, and stockpiling; refinement and acquisition of masks and improvements in air filtration systems to preclude infection via inhalation; improved intelligence collection and analysis; enhanced training; and the development of doctrine regarding how to preempt and, when necessary, respond to a biological attack.

An additional critical element of this program, however, is the need for an enhanced relationship between the military and those agencies charged with protecting the civilian population of the United States. In that regard, biological weapons necessarily alter our strategic thinking about national security and the nature of warfare. Wars may not always be fought on set-piece traditional battlefields, and it is time to throw away the anachronistic notion that the military's only role is to defend the United States against threats on foreign soil.

In the event of a domestic incident of biological weapons use, no matter who the perpetrator, it is unlikely that the response would be left to local law enforcement and health

officials or even to the Federal Bureau of Investigation, the Federal Emergency Management Agency, or the US Public Health Service. The military would undoubtedly be called on because of its resources, capabilities, and expertise. At the same time, if a biological incident were to occur in a military context, the Department of Defense would look to and need the help of such civilian agencies as the Centers for Disease Control and Prevention (CDC).

Although achieving it is one of our greatest challenges, an enhanced cooperation between military and civilian institutions is also likely to pay big dividends. In some respects the Atlanta Olympics were a good case in point, and the multi-agency partnerships that spanned federal, state, and local jurisdictions will serve as a model for future response.<sup>8</sup> Not only were the Olympics a model of cooperation, but they also marked a milestone for our response capabilities. In the immediate aftermath of the Centennial Park pipe-bomb explosion, bomb fragments were analyzed by Department of Defense assets—set up at a temporary laboratory at the CDC headquarters—to detect the presence of chemical or biological agents; none was found. This marked the first time that a domestic explosive had been routinely screened for those agents.

To facilitate and enhance this civil-military cooperation, Congress recently enacted the Defense Against Weapons of Mass Destruction Act of 1996, which seeks to enhance our domestic preparedness in several fundamental ways, including the following: by strengthening the federal government's ability to prevent and respond to terrorist incidents involving weapons of mass destruction; by enabling the Department of Defense and other federal supports to state and local prevention and response efforts; and by improving the capabilities of state and local emergency responders themselves. More than 100 cities in the United States have already been designated under the provisions of this legislation; their fire, police, rescue, and hospital emergency department personnel will receive training and equipment in an ambitious program conducted by the Department of Defense that began this summer.<sup>9</sup>

From another vantage point, the good news wrapped inside the particular problems posed by biological weapons is that in this arena, public health is the best form of civil defense. Our everyday domestic investments to detect and diagnose disease can and should be strengthened because of our national security trends. Biological weapons are not respectful of traditional boundaries of geography, bureaucracy, or conceptual compartmentalization. In that fact lies our challenge, our opportunity, and our call to action.

Richard Danzig, JD, DPhil  
 Pamela B. Berkowsky, MAlD

### References

1. Danzig R. Biological warfare: a nation at risk—a time to act. *Strategic Forum* [serial online]. January 1996.
2. Christopher GN, Cieslak TJ, Pavlin JA, Eitzen EM Jr. Biological warfare: a historical perspective. *JAMA*. 1997;278:412-417.
3. Vick K. Flea bargain rejected in bubonic plague case. *Washington Post*. April 2, 1996:A8.
4. Morgenthau T. A shadow over the Olympics. *Newsweek*. May 6, 1996:24.
5. Olson KB. Biological weapons and the terror in Japan. *Terrorism*. August 1997;11:1.
6. Beyerchen AD. From radio to radar: interwar military adaptation to technological change in Germany, the United Kingdom, and the United States. In: Williamson M, Millett AR, eds. *Military Innovation in the Interwar Period*. Cambridge, England: Cambridge University Press; 1996:285-292.
7. Zilmakos R. Iraq's biological weapons: the past as future? *JAMA*. 1997;278:418-424.
8. Tucker JB. National health and medical services response to incidents of chemical and biological terrorism. *JAMA*. 1997;278:362-368.
9. Horrocks M. The new terror fear: biological weapons: detecting an attack is just the first problem. *US News & World Report*. May 12, 1997:36.

Berger  
[Dick Clark]  
Lederberg  
Gorlick  
President

Shalala  
Reno  
Daley  
Holder

"Keeping America Secure for the 21<sup>st</sup> Cent."

10<sup>10</sup>

11<sup>20</sup> - 11<sup>45</sup> briefing

76 / 16.5

0010 / 15.5 / 48.5 / 8.0

SPEECH ON  
BIOLOGICAL/CHEMICAL AND CYBER TERRORISM

DATE: January 22, 1999

LOCATION: National Academy of Sciences

TIME: 10:10 to 11:00

FROM: SAMUEL BERGER

I. PURPOSE

Promote the Administration's efforts to combat the emerging threats of biological/chemical and cyber terrorism.

II. BACKGROUND

This event follows your Thursday interview with the *New York Times* on the same subject. Your remarks will highlight new 21<sup>st</sup> century threats and announce your FY00 initiatives to combat them.

You have a strong record on these issues. Last May you announced two new PDDs on counter-terrorism, weapons of mass destruction preparedness and critical infrastructure protection, and named the first-ever National Coordinator, Richard Clarke. Shortly thereafter, you submitted the budget supplemental for biological and chemical weapons preparedness. Your FY00 budget shows a substantial increase in spending on new programs to combat unconventional threats: over a two-year period, you will have nearly doubled funding for programs to prepare for CBW terrorism, raising it to \$1.33 billion. You are also proposing a one-year increase of \$400 million for critical infrastructure protection, raising it to \$1.46 billion.

In your remarks at the National Academy of Sciences, you will announce that this money will help pay for several FY00 initiatives. To help defend against biological or chemical terrorism, you will announce four initiatives. A new medical R&D effort will focus on developing vaccines and medicines for likely bioterrorism agents. Upgrades to the public health system will help doctors and other medical workers recognize a biological attack, diagnose the

agent, and respond rapidly. National assets including National Guard, Army, Marines and Coast Guard CBW units will be improved to assist local emergency responders if necessary. And the National Domestic Preparedness Office in the Justice Department will help create a national contingency plan for 120 metropolitan areas and provide a single, integrated federal program to train and equip the first responder community across the country.

You will also announce four initiatives on cyber terrorism. A Computer Security Applied Research Initiative will focus on developing new intrusion detection systems and methods for detecting malicious code installed by unauthorized users. Beginning with the Defense Department, we will build a government-wide system of Computer Intrusion Detection Networks to warn and defend all computers against cyber attack. Seed money will be available to stand up Information Sharing and Analysis Centers to facilitate genuine public-private partnerships on critical infrastructure protection. And finally, we will set up the administrative structures for Cyber Corps, a program to address the acute shortage of highly trained computer experts in the Government. This last program may evolve into a ROTC-like program to trade computer science scholarships for a commitment to government service.

### III. PARTICIPANTS

Speakers: POTUS, Berger, Josh Lederberg and Jamie Gorelick. Lederberg, a Nobel Laureate at Rockefeller University, will make remarks on threat of bioterrorism (he was also a member of your roundtable on biological weapons last year). Gorelick is co-chair (with Sam Nunn) of the Advisory Council to the President's Commission on Critical Infrastructure Protection and will make remarks about the threat of cyber terrorism. We expect some cabinet members to attend: Reno, Shalala, Richardson and Daley.

### IV. PRESS PLAN

Press briefing prior to event by Reno, Shalala, Daley and Richard Clarke. Open press at the event. After the event, press moves to nearby room filled with static displays of CBW equipment. Then press is led outside to view CB decontamination truck, similar to the one we will supply to 120 cities. Concurrently, selected press will be scheduled interviews with selected validators.

V. SEQUENCE

Press briefing. Clarke and I brief you. Travel to National Academy of Sciences. I make brief introductory remarks (3 minutes). Josh Lederberg speaks on the bioterrorism threat (5 minutes). Jamie Gorelick speaks on the cyber terrorism threat (5 minutes). Your speech (12 minutes). No questions from the press. Work the room briefly, then depart. Presentations continue for press.

Attachment

Tab A Presidential Remarks

**Wechsler, William F.**

---

**From:** Halperin, David E.  
**Sent:** Wednesday, January 20, 1999 3:09 PM  
**To:** Halperin, David E.; @TRANSNATIONAL - Transnational Threats; Bernard, Kenneth W.; @INTECON - Economic Affairs; @LEGAL - Legal Advisor; @LEGISLAT - Legislative Affairs; @RUSSIA - Russia/Ukraine; @PLANNING - Strat Plan & Comm; @NONPRO - Export Controls; @NESASIA - NE/South Asia; @AFRICA - African Affairs; @DEFENSE - Defense Policy; @EUROPE - European Affairs; @INTEL - Intelligence Programs  
**Cc:** Hachigian, Nina L.; Sutphen, Mona K.  
**Subject:** RE: POTUS Friday terrorism remarks [UNCLASSIFIED]

Latest draft -- reflecting input from many of you -- attached. If you haven't looked yet, start here. Those who are on the peripheries of this topic and who reviewed the previous draft can, of course, ignore this round.



new threats 1-99.doc

-----Original Message-----

**From:** Halperin, David E.  
**Sent:** Wednesday, January 20, 1999 9:58 AM  
**To:** @TRANSNATIONAL - Transnational Threats; Bernard, Kenneth W.; @INTECON - Economic Affairs; @LEGAL - Legal Advisor; @LEGISLAT - Legislative Affairs; @RUSSIA - Russia/Ukraine; @PLANNING - Strat Plan & Comm; @NONPRO - Export Controls; @NESASIA - NE/South Asia; @AFRICA - African Affairs; @DEFENSE - Defense Policy; @EUROPE - European Affairs; @INTEL - Intelligence Programs  
**Cc:** Hachigian, Nina L.; Sutphen, Mona K.  
**Subject:** POTUS Friday terrorism remarks [UNCLASSIFIED]

Draft for POTUS terrorism remarks, to be delivered Friday 10:10 am. Please provide comments to me by 4 pm today or sooner. Needs to go to SRB/JBS by 6 pm today and to WH staff ASAP tomorrow. Thanks. David << File: new threats 1-99.doc >>

1/20/99 3:00 p.m.

Halperin

69371

Will Wexler  
69351

9366

**PRESIDENT WILLIAM JEFFERSON CLINTON**  
**REMARKS ON KEEPING AMERICA SECURE IN THE 21<sup>ST</sup> CENTURY**  
**WASHINGTON, DC**  
**JANUARY 22, 1999**

**Acknowledgments**

For more than 220 years, America has met the challenge of defending our nation against those who would do us harm. We have done so by drawing on the very best of our society -- the skill and courage of our armed forces, but also the genius of our scientists and engineers, the dedication and strength of our factory workers, the vision of leaders in every vital sector.

And from the beginning, we have addressed our security challenges confident that our cause is just. It is the cause of freedom and democracy and human dignity.

Today, with a new millennium only months away, our ideals are closer than ever to realization. We are working harder than ever here at home for deeper democracy, racial and religious tolerance, and equal opportunity. And around the world, often with America's help, people are freeing themselves from tyranny and old hatreds and embracing reconciliation and liberty.

We can see before us a new era, one where nations unite for stronger schools, better health care, broader prosperity, a cleaner environment, and greater participation by citizens in shaping their futures.

But the struggle to defend our people and our values -- the struggle to make this better world possible -- is not over. Open borders and a revolution in technology have spread the message and the gifts of freedom, but they have also given new opportunities to freedom's enemies -- terrorists and outlaw nations who want to undermine the world's progress.

Last August, at Andrews Air Force base, I met with the families of the brave and dedicated Americans who lost their lives at our embassy in Kenya. We grieved together as their loved ones returned home. They were in Africa to promote the interests and values that America shares with friends of freedom around the world. For that, they were murdered by terrorists. Men and women at the Oklahoma City federal building, at the World Trade Center, at Khobar Towers in Saudi Arabia, on Pan Am 103 -- they were murdered by terrorists, too.

Exactly eight months ago, at the United States Naval Academy, I warned that our adversaries were extending the fields of battle -- from physical space to cyberspace, from the world's vast bodies of water to the complex workings of our own human bodies.

These enemies know they cannot defeat us by traditional military means. So they are working on new forms of attack. First, they may attempt cyber-attacks: using computers to disable power grids, banking and communications networks, transportation systems, police, fire, and health

services, and military structures. These critical systems are increasing linked together and increasingly dependent on computers for their operation. This greatly increases our productivity but also makes us much more vulnerable to disruption.

Second, our enemies may seek to attack us with compact and relatively inexpensive weapons of mass destruction: biological weapons, which use disease as an instrument of war, chemical weapons, even nuclear weapons.

As the previous speakers have made clear, our concerns are not based on conjecture. Attacks on our critical systems already are underway. Hackers break into government and business computers, raiding banks, running up credit card charges, extorting money by threats to unleash computer viruses. And terrorists have already obtained weapons of mass destruction. Four years ago, a terrorist group unleashed deadly nerve gas in the Tokyo subway. Twelve people died, and thousands were injured.

Still, I want to stress that, today, there are serious obstacles to deter and prevent terrorist groups from mounting successful cyber attacks or acquiring and using mass destruction weapons. Most victims of terror today fall to the same bullets and bombs that terrorists wielded a hundred years ago. But we are taking action now against the new threats because we know that, when it comes to defending our people, we must remain ahead of the curve. We must be ready to address these emerging threats while it is still possible to thwart them.

We are already moving to meet these challenges. We are pressing ahead with arms control initiatives: to strengthen compliance with the Biological Weapons Convention and adherence to the Chemical Weapons Convention ... to end production of nuclear weapons material ... and to ratify a Comprehensive Test Ban Treaty that will end nuclear tests once and for all. With verifiable agreements to keep nations from acquiring these weapons, we can help keep them out of the hands of terrorists, too. As I announced Tuesday in my State of the Union address, we are also intensifying efforts to help Russia and other former Soviet states prevent weapons materials and knowledge from going to terrorists and outlaw nations.

We have improved anti-terrorism cooperation with other countries; tightened security for our diplomats, troops, and air travelers; and strengthened sanctions on nations that support terrorists. Since 1993, we have tripled funding for FBI efforts to fight terrorism. Our law enforcement agencies have done extraordinary work in tracking down perpetrators of terrorist acts and bringing them to justice. Meanwhile, our armed forces are prepared to strike against weapons of mass destruction facilities, as we did last year in Iraq and Sudan.

In my Naval Academy address eight months ago, I announced new initiatives to address these emerging security challenges. And I named Richard Clarke our National Coordinator, to marshal the efforts of all parts of our government. Today, I can report that we are making substantial progress. In particular, we are increasing our readiness in the event of an attack -- so we can protect our citizens and our vital assets. And so we can show the terrorists that attacks on America will serve no purpose other than bringing their own downfall.

Already, we have created special offices within the FBI and the Commerce Department devoted to protecting our critical systems against cyber attack. Because so many key parts of our society are operated by the private sector, we are working to create a genuine public-private partnership: to find and reduce vulnerabilities to cyber attack ... to develop warning systems that will alert us to attacks ... to minimize damage and rapidly recover if attacks occur.

I obtained from Congress a substantial budget increase for chemical and biological weapons preparedness. We have launched efforts to train and equip fire, police and medical personnel across the country to deal with chemical and biological emergencies ... to ready armed forces and National Guard units in every region to meet this challenge ... to build a robust public health surveillance system -- so that if a biological weapon or other source of disease is released, we can detect it and save lives ... to create the first-ever civilian stockpile of needed medicines ... to increase research on new medications.

Our commitment to give local communities the necessary tools already goes far beyond paper and plans. Parked just outside this building is a newly-designed truck with the capacity to rapidly assist and prevent harm to people exposed to chemical and biological dangers. We have provided it to the Arlington, Virginia, Fire Department to serve the Washington, D.C., area. We will send similar vehicles to 120 metropolitan areas throughout the country.

Our troops on the frontlines need protection, too. So we are working to vaccinate them against biological threats, including deadly anthrax bacteria.

But we must do even more to meet these threats. So today I want to announce further initiatives aimed at these threats -- to keep America secure in the new century.

*bioterrorism  
initiation  
breakout*

In my new budget, I will ask Congress for approximately \$10 billion to address terrorism and terror's emerging tools. This will include nearly \$1.4 billion for our efforts to protect citizens against chemical and biological terror -- more than double what we spent on such programs only two years before. We will speed and broaden our efforts for emergency response and attack detection. And we will greatly accelerate research and development for new medicines, vaccines and diagnostic tools. This effort will address not only the threat of mass destruction weapons but also the equally serious threat of emerging infectious diseases. Let me add that at the NATO summit here in April, we hope to make progress to better equip our allies to address chemical and biological threats.

Our budget proposal will also include \$1.46 billion to protect our critical systems from cyber and other attacks. And on the cyber front, I want to announce four new initiatives. First, we will launch an intensive research effort to detect cyber intruders who try to break in to critical systems and insert computer viruses. Second, we will create Intrusion Detection Networks, first for our Defense Department and later for other key agencies -- so when one critical computer system is attacked, others will be alerted instantly. And we will urge the private sector to create similar structures. Third, we will support the establishment of Information Sharing and Analysis Centers in the private sector, so our industries will work together, and with government, to address common security challenges. Finally, we will ask for authority to design and launch a new program offering college scholarships in computer science in exchange for federal service

helping to safeguard government computers. This new Cyber Corps will reduce our shortage of qualified computer experts, increase the quality of computer education, and help young people of modest means enter our most promising fields.

In all our efforts to battle terrorism, cyber-attacks, and weapons of mass destruction, we will be aggressive. But let me be very clear: We must and we will continue to uphold privacy rights and other constitutional protections, as well as the proprietary rights of our industries. It is absolutely essential that we do not undermine liberty in the name of liberty.

The challenges we face are great, but we can meet them. At the end of this century, as freedom's enemies have grown more dangerous, freedom's promise has grown stronger. The conflict has been heightened, the stakes have been raised, but the essential task is the same one Woodrow Wilson described more than eighty years ago: "The world must be made safe for democracy." To do so, we must, as we have done so effectively in the past, draw on our science and technology sectors, our industry, and our government agencies, in a unified effort. Together we can protect our citizens and fulfill our dreams for a future of progress and prosperity. Thank you very much.

###



## **FAX Transmission**

**U.S. Department of Health and Human Services  
Office of the Secretary**

**DATE:**

**TO:**

*Devora*

**FAX:**

**PHONE:**

**FROM:**

Ellen Dahl

Office of the Assistant Secretary for Public Affairs

Phone: (202) 690-7578

Fax: (202) 690-5673

**TOTAL NUMBER OF PAGES TRANSMITTED:**

**COMMENTS:**

THU 13:49 FAX 202 456 9360

2

- The first ever civilian medical stockpile, which will contain necessary medication to treat those exposed to biological or chemical weapons.
- Upgrading of the public health surveillance system, so medical personnel can detect a biological weapons release early, thus saving lives.

### NEW BUDGET PROPOSALS

The 2000 budget builds on the progress thus far and includes major increases in resources for preparedness.

- HHS will receive an additional \$40 million for R&D in this area – more than a 140% increase. The bulk of it – \$30 million – will go to research on new vaccines, including for smallpox and anthrax for eventual use in the national medical stockpile.
- Funding for improvements in the public health surveillance system will rise by 23% to \$87 million. This will translate into increased lab capacity, strengthened epidemiological capabilities for state and local health departments and more resources for communications and information technology. The Center for Disease Control will create a network of ~~12~~ major labs to provide rapid analysis of select biological agents. *+ Prevention*
- Funding for Metropolitan Medical Response Systems – the local emergency medical teams to respond to a biological or chemical weapons emergency – will be dramatically increased by more than 300% to more than \$24 million. Twenty five new such teams will be funded.

**HHS BIOTERRORISM, FY 2000 -- For W.H. Factsheet*****"Problem" section:***

While the likelihood is unknown, the possible use of biological weapons by terrorists could inflict life-threatening illness on a large scale. Even a lone terrorist could cause disease in a significant population group -- and in the case of communicable disease, the illness could spread in successive waves of infection. Yet, unlike explosions or chemical releases, a bioterrorist attack could be surreptitious, and thus difficult and time-consuming to detect. Symptoms might not occur among victims for days or weeks, and those initially presenting themselves to physicians and clinics would not all be in one place. A strong public health network would be needed to piece together early reports and determine quickly what had happened. And once detected, the situation could overwhelm traditional local health systems, faced not only with the tasks of caring for mass casualties but also with the demands of even larger numbers of the "worried well" for treatment or vaccination.

***"Proposal" section:***

HHS is acting rapidly to build a stronger base to be prepared for possible bioterrorist attacks. The HHS initiative relies heavily on cooperation with state and local health agencies as well as local emergency response units. The President will propose \$230 million for the HHS initiative in FY 2000, up from \$158 million this year. HHS efforts are directed especially at:

- Strengthening disease surveillance and the public health network -- Working with states, HHS will improve disease surveillance and lab capacity to detect outbreaks. HHS will also invest in improved information technology for the public health network so that findings can be reported and shared faster.
- Medical and public health response -- HHS will work with local governments to expand the capacity for responding to bioterrorist and other unconventional emergencies. HHS has helped 27 local areas so far in creating Metropolitan Medical Response Systems, with up to 20 more to be created this year. Ultimately 120 of these local systems are to be created across the nation.
- National pharmaceutical stockpile -- A new stockpile will be created to assure that the volume and range of needed pharmaceuticals can be made available quickly. Initial focus will be on anthrax, smallpox, pneumonic plague and tularemia.
- Research -- HHS will support expanded research to better understand likely bioterrorism disease agents, including genome sequence information. The effort will also aim at developing new vaccines and other drugs as well as new, more effective techniques for detection of organisms used in a bioterrorist attack.

## THE WHITE HOUSE

## Office of the Press Secretary

For Immediate Release

January 22, 1999

**DRAFT****FACT SHEET**

**Keeping America Secure for the 21<sup>st</sup> Century:  
President Clinton's Initiative on  
Biological and Chemical Weapons Preparedness**

President Clinton has made defending the United States against chemical and biological weapons a top priority of his national security strategy. The possibility that outlaw nations and terrorist groups will seek to use these weapons against us represents one of the greatest threats to American security in the 21<sup>st</sup> century. The Administration has sought to defend against these threats through diplomatic and military means abroad and through increasing preparedness at home. In his Fiscal Year 2000 budget - which includes \$10 billion to defend against terrorism and weapons of mass destruction -- President Clinton proposes major increases in funding to strengthen America's defenses against the threat of biological and chemical weapons.

- **Vaccine Research and Development** - The Department of Health and Human Services will receive an additional \$43.4 million for research and development to defend against biological weapons - almost a 150% increase. The bulk of it - \$30 million - will go to research on new vaccines, including vaccines for smallpox and anthrax for eventual use in the national medical stockpile. The Federal Drug Administration will receive \$13.4 million for expedited regulatory review of vaccines and therapeutics. [In addition, the National Institutes of Health will receive \$24 million - as it did last year - for research on diagnostics, vaccines, antimicrobials and genomic research.]
- **Public Health Surveillance** - President Clinton will propose that funding for improvements in the public health surveillance system and public health infrastructure increase by 22% to \$86 million. This will translate into increased lab capacity, strengthened epidemiological capabilities for state and local health departments and more resources for communications and information technology. The Center for Disease Control will create a network of regional labs

**DRAFT**

provide rapid analysis and identification of select biological agents.

- **Metropolitan Medical Response Systems** - President Clinton will propose increasing funding by almost 400% to more than \$16 million for Metropolitan Medical Response Systems. These local emergency medical teams to respond to a biological or chemical weapons emergency. Twenty-five new such teams will be funded.

President Clinton's new initiatives build upon a record of accomplishment in confronting the dangers of emerging threats at home and abroad.

- Beginning in fiscal 1997, the Administration began funding a five-year effort to equip and train first responders in the 120 largest metropolitan areas in the nation.
- Last year, the President proposed and Congress approved of more than \$300 million in additional funds for weapons of mass destruction preparedness. [Among the initiatives begun were the renovation of the public health surveillance system so medical personnel can detect a biological weapons release early and save lives. This appropriation also went to establish the first ever civilian medical stockpile, which will contain necessary medication to treat those exposed to biological or chemical weapons. (Funding for the medical stockpile will be maintained in the President's FY2000 budget.)]
- The United States led international efforts to ratify the Chemical Weapons Convention, which we signed in 1997, and American diplomats are currently working to strengthen the Biological Weapons Convention.
- The Clinton Administration has also pursued an aggressive policy of cooperative threat reduction with nations of the former Soviet Union, spending \$30 million during the last five years on reducing the threat from biological weapons. The President's budget proposal seeks more than \$150 million to expand these efforts over the next five years.
- Through military action against production facilities for weapons of mass destruction in Iraq and Sudan, the United States has acted to degrade and eliminate the ability of these two nations to build weapons of mass destruction and supply them to terrorists.

757-5000



U.S. Department of Justice  
Office of Justice Programs

Office for State and Local Domestic  
Preparedness Support  
810 7th Street, NW  
Washington, DC 20531  
Phone: (202) 305-9887  
Fax: (202) 616-2922

**FACSIMILE TRANSMISSION  
COVER SHEET**

*ATTN*  
TO: Devora Adler  
OFFICE: W/H Domestic Policy Office Council  
TELEPHONE NO.: \_\_\_\_\_ FAX#: 456-~~5557~~ 5557  
PAGES: 15 (Includes cover sheet) DATE: 3/1/99

FROM:

Andy Mitchell

TELEPHONE NO.:

305-9889

NOTES: Info on OJP's FY99 Program Plan  
as discussed (ps. 2-12) plus 3pg overview of  
OSDPS Program History-

Please let me know if you have any questions-

Andy Mitchell

**Office for State and Local  
Domestic Preparedness Support**

**Fiscal Year 1999  
First Responders Equipment Acquisition Program  
(\$69.5 million)**

**Background:**

As a part of the Office of Justice Programs first responder domestic preparedness initiative, the Conference Report (H. Rpt. 105-825 p. 998) accompanying the Justice Department's Fiscal Year 1999 appropriations Act provides \$75.5 million to ensure that first responders are properly equipped and prepared to respond to incidents of domestic terrorism involving chemical and biological agents,, as well as radiological and explosive devices. Pursuant to the Conference Report language, equipment acquisition assistance will be provided to the nation's 157 largest cities and localities, as well as the States.

**Program:**

Of the \$75.5 million, \$69.5 million will be used to provide personal protective gear, and detection, decontamination, and communications equipment to first responders; \$4 million is for the purchase of equipment for the National Domestic Preparedness Consortium (per instructions of the Conference); and \$2 million is for transfer to the Office of Justice Programs for management and administration per instructions of the Conference).

The First Responder Equipment Acquisition Program will provide \$69.5 million in grants to the 157 largest cities and localities, as well as the States, to procure personal protective, chemical/biological detection, decontamination, and communications equipment. This equipment will enable fire departments, law enforcement agencies, emergency medical services, hazardous materials response units, and other emergency response agencies to enhance their response capabilities to incidents of domestic terrorism. The design and implementation of this program will be coordinated with the National Domestic Preparedness Office (NDPO) within the Federal Bureau of Investigation (FBI). The Standardized Equipment List (SEL) jointly developed by the DOD and the FBI, will be a critical component of OJP's Application Kits developed for this program. The Application Kit, originally developed for the FY 1998 Equipment Grant Program in cooperation with the FBI, will be reviewed and finalized for both components of the FY 1999 Program in cooperation with the NDPO.

**PART I**

Of the \$69.5 million, approximately \$46 million will be provided to the 157 largest cities and localities, which will be divided into three award categories. The number of jurisdictions in each category will be based on population. Those cities and counties with the highest populations will receive the largest awards, and those with the lowest populations the smallest awards. A breakdown of the preliminary award amount categories and number of jurisdictions is as follows:

First Responder Equipment Acquisition Program (PART I contd.)

\$450,000 (50 jurisdictions) = \$22,500,000

\$200,000 (50 jurisdictions) = \$10,000,000

\$125,000 (57 jurisdictions) = \$ 7,125,000

Total = \$45,525,000

PART II

The remaining approximately \$24 million will be provided to the 50 States. A baseline amount of \$250,000 will be allocated to with the balance distributed to the states on a population share basis. Governors will be contacted to designate an agency to administer the program.

## FIRST RESPONDER EQUIPMENT ACQUISITION PROGRAM

### TIME LINE:

**August 15, 1999** — Grant awards made. Grant award documents must be signed out in order to allow time for final Comptroller review, Congressional notifications, and announcements prior to the September 15, 1999 cut-off date for Office of the Comptroller grant processing for FY 1999.

**July 1, 1999** — Decisions on grant recipients and awards made. Allows time for contacts back with grantees to settle any financial or programmatic issues requiring resolution; for Comptroller Office review of proposed budgets for allowable costs, etc.; and for preparation of grant award packages.

**May 15, 1999** — Deadline for OJP receipt of applications. Allows for OJP staff review, peer review, and preparation of recommendations to the AAG.

*Revised* → **March <sup>30</sup> 15, 1999** —

Grant solicitation document released to the field for state and local jurisdictions to have time to prepare and submit their proposals.

*Tentative* → **Mid March** —  
**February 1, 1999** —

(Governors asked to designate agency to apply for state grants)  
Decision/consensus must be reached through NDPO or others as required on (a) an equipment list; (b) jurisdictions that are eligible under the Appropriations Act; (c) any other predicate criteria that may be imposed; and (d) time allowed for drafting and circulation of the draft solicitation document.

**Office for State and Local  
Domestic Preparedness Support**

**Fiscal Year 1999  
Municipal Fire and Emergency Services Equipment Program  
(\$20 million)**

**Background:**

As part of the Office of Justice Programs' (OJP) first responder domestic preparedness initiative, the Conference Report (H. Rpt. 105-825 p. 998) accompanying the Justice Department's Fiscal Year 1999 Appropriations Act provides \$25 million to expand equipment and training programs targeted specifically to municipal fire and emergency services departments.

**Program:**

Of the \$25 million, \$16 million is was earmarked to assist municipal fire and emergency medical services departments to acquire equipment; \$4 million was earmarked for interoperable radio equipment for local emergency response agencies; and \$5 million was earmarked for training for these same agencies. As the \$16 million equipment program is integrated with the \$69.5 million equipment acquisition program, the planning for its implementation will also be coordinated with the NDPO, and the NDPO SEL will be incorporated into the application package.

**Municipal Fire and Emergency Services Equipment Acquisition Program**

**Part I:**

This program component will provide \$7.5 million in grants to the remaining 55 cities which have been designated for training under the Nunn-Lugar-Domenici Domestic Preparedness Program that are not eligible for funding under OJP's FY 1999 69.5 million First Responder Equipment Acquisition Program. Grants up to \$125,000 will be awarded to each of the 55 jurisdictions.

**Part II:**

Of the remaining funds, \$4.3 million will be available to the state capitols not receiving grants under the First Responder Equipment Program or the above Part I program, and the largest cities and state capital in those 12 states not reached by the FY 1999 First Responder Equipment Acquisition Program. This approach will address one of the major deficiencies of both DOD and OJP's current program targeting lists by reaching the 12 states currently not served through either program. Grants up to \$100,000 will be awarded to each of these 43 jurisdictions.

Municipal Fire and Emergency Services Interoperable Communications Equipment Program

Through a joint initiative with the National Institute of Justice's Office of Science and Technology, OJP will conduct an assessment of new communications equipment designed to help address the interoperable communication problem facing state and local agencies. Tests of equipment will be conducted in 10-12 cities and, if proven successful, the technology, at a cost of \$25,000 to \$30,000 per site, will be made available to approximately 140 jurisdictions around the country from the \$4 million available for this program.

## MUNICIPAL FIRE AND EMERGENCY SERVICES EQUIPMENT ACQUISITION PROGRAM

### TIME LINE:

- August 15, 1999** -- Grant awards made. Grant award documents must be signed out in order to allow time for final Comptroller review, Congressional notifications, and announcements prior to the September 15, 1999 cut-off date for O.P. grant processing for FY 1999.
- July 1, 1999** -- Decisions on grant recipients and awards made. Allows time for contacts back with grantees to settle any financial or programmatic issues requiring resolution; for Comptroller Office review of proposed budgets for allowable costs, etc.; and for preparation of grant award packages.
- May 15, 1999** -- Deadline for OJP receipt of applications. Allows for OJP staff review, peer review, and preparation of recommendations to the AAG.
- March 15, 1999** -- Grant solicitation document released to the field for state and local jurisdictions to have time to prepare and submit their proposals.
- February 1, 1999** -- Decision/consensus must be reached through NDPO or others as required on (a) an equipment list; (b) jurisdictions that are eligible under the Appropriations Act; (c) any other predicate criteria that may be imposed; and (d) time allowed for drafting and circulation of the draft solicitation document.

**MUNICIPAL FIRE AND EMERGENCY SERVICES  
INTEROPERABLE COMMUNICATIONS EQUIPMENT PROGRAM**

**TIME LINE:**

**May 15, 1999** -- Application kits distributed or Federal Register announcement made for computer application.

**April 30, 1999** -- NIJ assessment completed. Final report published.

**Mid-February 1999** -- Applications for demonstration sites awarded. *- This step behind schedule - likely 4/1 @ earliest.*

**Mid-January 1999** -- Convene meeting of demonstration sites to review requirements for test participation, time line for NIJ assessment, and application requirements.

**Office for State and Local  
Domestic Preparedness Support**

**Fiscal Year 1999**

**State and Local Domestic Preparedness-First Responder Training Program  
[\$16 million]**

**Background:**

As part of OJP's first responder/domestic preparedness initiative, the Conference Report (H. Rpt. 105-825, pp. 998-999) accompanying the Justice Department's Fiscal Year 1999 Appropriations Act, provides \$16 million to provide training to state and local emergency response personnel (first responders and other emergency personnel) to enhance their capability to respond to incidents of domestic terrorism involving chemical and biological agents and radiological and explosive devices.

**Program:**

This training will be carried out through the National Domestic Preparedness Consortium which is comprised of OJP's Center for Domestic Preparedness, located at Fort McClellan, Alabama; the National Energetic Materials Research and Testing Center located at the New Mexico Institute of Mining and Technology; the National Center for Bio-Medical Research and Training located at the Louisiana State University; the National Emergency and Response and Rescue Training Center located at the Texas A&M University; and U.S. Department of Energy's National Exercise, Test, and Training Center (Nevada Test Site). Coordination of program development and execution will be coordinated with the Training Program Section of the National Domestic Preparedness Office to ensure coordination across the Federal interagency family and to leverage existing training curricula which can be modified or integrated into the Consortiums training program.

The National Domestic Preparedness Consortium was formally organized on June 11, 1998 in order to bring together the various entities receiving funding under OJP's domestic preparedness initiative into a singular, coordinated, and integrated training program. OJP's Center for Domestic Preparedness (CDP) at Fort McClellan, Alabama was formally established as an OJP component on June 1, 1998. The CDP operates as part of OJP's Office for State and Local Domestic Preparedness Support.

OJP's domestic preparedness training program will: 1) identify the training needs of the emergency response community both by discipline (law enforcement, fire service, etc.) and by personnel level within those disciplines (fireman, HAZMAT technician, etc.); 2) identify existing and/or develop curricula to meet those training needs; 3) evaluate and standardize training curricula with the assistance of experts from the field; 4) deliver training both locally (through on-site or distance learning capabilities) and at specialized training facilities (such as the CDP at

### **State and Local Domestic Preparedness-First Responder Training Program (cont.)**

Fort McClellan) for more advance training; 5) review and modify training to meet new needs, new technologies, or new threats; and 6) identify emergency response personnel and match them to proper training courses based on their individual and their communities' needs.

Although training needs will be further identified through the OJP Needs Assessment of State and Local Jurisdictions, much is already known about the type of training required by many in the emergency response community. Further, there are a number of existing training curricula geared for various levels and types of emergency response personnel. Much of this exists within (and has been identified by) the expertise and resources of the National Domestic Preparedness Consortium. During Fiscal Year 1999 the Consortium will focus on the identification of training needs, the development of training courses and the delivery of courses to emergency response personnel in four major areas: 1) Awareness, 2) Responder Operations, 3) Technician Response, 4) Weapons of Mass Destruction Incident Management. Within each of these areas several different course will be taught. Each Consortium member will be responsible for the delivery of a different set of courses depending on their expertise and facilities. [A chart listing specific courses within these areas and the Consortium member responsible for their delivery is attached.]

Per the instructions of the Conference Report, OJP will provide \$2 million (each) to the New Mexico Institute of Mining and Technology, the Louisiana State University, the Texas A&M University, and the Nevada Test Site (through the Department of Energy). Each of these sites will also receive an additional \$1 million (per instructions of the Conference Report to be taken from the First Responder Equipment Acquisition Program) to purchase equipment associated with their training of emergency response personnel. The CDP at Fort McClellan will receive \$8 million to support both its operations cost (as an OJP facility) and to support first responder training.

To ensure coordination of OJP's domestic preparedness training program, OJP staff and Consortium representatives meet on a frequent and regular basis and maintain weekly, if not daily, communication. Both OJP and the Consortium members see the Consortium as an entity that can provide leadership, expertise, and resources to the emergency response community on a nation wide level. To this end OJP will also provide technical assistance funds to the Consortium to support its development and outreach to the emergency response community. OJP is coordinating its entire training program with the NDPO, and other Federal agencies, state and local agencies, and the emergency response community.

**State and Local Domestic Preparedness-First Responder Training Program (cont.)****Time Line:**

March 15, 1999

Consortium development and support funds awarded.

March 15, 1999

Training and Equipment Support funds awarded.

December 21, 1998

Consortium proposals and budgets received.

Note: Meetings of Consortium representatives are scheduled monthly. NDPO staff will be invited to participate in these meetings. Planning and development of training programs and Consortium activities are continuous and ongoing.

**Office for State and Local  
Domestic Preparedness Support**

**Fiscal Year 1999  
State and Local Situational Exercise Program  
[\$3.5 million]**

**Background:**

As part of OJP's first responder training/domestic preparedness initiative, the Conference Report (H. Rpt. 105-825, p. 999) accompanying the Justice Department's Fiscal Year 1999 Appropriations Act provides \$3.5 million for situational exercises for state and local emergency response personnel.

The Conference language further directs that a portion of these funds be used to comply with language found in the Senate Report (S. Rpt. 105-235 ) requiring that a "Topoff" exercise be included under any exercise initiative. Under the Senate Report, two types of exercises are discussed. The first is a major, national level "topoff" exercise. The other is to incorporate situational exercises as part of OJP's efforts to improve the capabilities of state and local emergency personnel respond to incidents of domestic terrorism (see page 12).

Similar language is found in the House Reports (H.Rpt. 105 - 636, at 13 ) which directs the use of "confidence building exercises based on threat driven scenarios" be incorporated into OJP's training efforts.

**Program:**

Program development on hold pending OMB decision on which agency should administer this program.

**Office of Justice Programs  
Office for State and Local Domestic Preparedness Support**

**Improving State and Local Response Capabilities**

**Overview:**

Based upon a delegation by the Attorney General, the Assistant Attorney General for the Office of Justice Programs (OJP) has responsibility for the administration of the the Justice Department's state and local domestic preparedness assistance programs for the purpose of enhancing the capabilities of state and local jurisdictions respond to incidents of domestic terrorism including incidents involving chemical and biological agents and nuclear and explosive devices.

**Legislative History:**

The Fiscal Year 1998 Appropriations Act, [ Pub.L. 105-119], signed November 26, 1997, provided \$16,000,000 under the Counterterrorism Fund for three purposes: 1) \$12,000,000 to provide grants for acquisition of terrorism-related equipment for state and local agencies; 2) \$2,000,000 for support operations of the state and local training center for First Responders at Fort McClellan, Alabama; and 3) \$2,000,000 for operations of a similar training center at the New Mexico Institute of Mining and Technology.

The Conference Report [H. Rpt. 105-405] which accompanied the FY 1998 Appropriations Act provided more detailed guidance and directs the Justice Department to develop and implement a coordinated effort to enhance state and local capabilities to respond to incidents of domestic terrorism. The Conference Report directs the implementation of four (4) new initiatives. The first, establishes a program to assist state and local jurisdictions in purchasing equipment needed to respond to terrorist incidents. The second is to establish a specialized training facility for state and local First Responder at Fort McClellan, Alabama. The third is to provide additional training by utilizing the facilities at the New Mexico Institute of Mining and Technology in Socorro, New Mexico. The fourth is to provide additional assistance to state and local first responders through the facilities of the Texas A&M University's National Emergency Response and Rescue Training Center and through the Nevada Test Site.

There is strong Congressional support for these domestic preparedness initiatives, particularly on the part of the Senate. A principal supporter is Senator Judd Gregg (R-NH) who chairs the Justice Department's Appropriations Subcommittee. Other Senate supporters include: Senator Jeff Bingaman (D-NM), Senator Paul Coverdale (R-GA), Senator Pete Domenici (R-NM), Senator Kay Bailey-Hutchinson (R-TX), Senator Harry Reid (D-NV), Senator Jeff Sessions (R-AL), and Senator Richard Shelby (R-AL).

### **The Office for State and Local Domestic Preparedness Support:**

On April 30, 1998, the Attorney General signed the delegation of authority designating the Assistant Attorney General for the Office of Justice Programs (OJP) as the Justice Department official responsible for the implementation and administration of these initiatives. OJP's long history and experience working with state and local jurisdictions provides the knowledge and infrastructure to effectively and efficiently administer these programs.

Immediately thereafter the Office of Justice Programs (OJP) proposed the establishment of the Office for State and Local Domestic Preparedness Support (OSLDPS) as a component within the Office of the Assistant Attorney General for OJP. Also included within the proposed office was OJP's existing Metropolitan Firefighter and Emergency Medical Services Training Program which since its inception in 1997 had been administered by OJP's Bureau of Justice Assistance.

On August 21, 1998, the Attorney General approved the reorganization plan and officially established OSLDPS as an OJP component located within the Office of the Assistant Attorney General/OJP. The Director, OSLDPS, reports directly to the Assistant Attorney General/OJP.

Under OJP, OSLDPS' mission is to:

- Provide financial assistance (grant funding) to enable state and local jurisdictions buy the equipment needed to respond to incidents of domestic terrorism.
- Offer a broad spectrum of training, including the use of field exercises, to ensure that state and local emergency response personnel (including law enforcement, fire and emergency medical services, public works, public health, state and local officials, and others) have the skills, knowledge, and abilities to respond well if incidents of domestic terrorism occur.
- Offer technical assistance to provide guidance, advice, and share the information required to make the critical decisions domestic preparedness requires.

Since the Attorney General signed the delegation of authority vesting responsibility for these efforts within OJP, OSLDPS' has:

- Developed, designed and implemented the "State and Local Domestic Preparedness Equipment Support Program" to distribute the \$12 million appropriated in FY 1998 to local jurisdictions to assist in the purchasing of equipment needed to respond to incidents of domestic terrorism. On September 18, 1998, grant awards ranging from \$117,686 to \$500,000 were awarded to 41 jurisdictions across the nation. Out of 120 jurisdictions eligible under this competitive grant program, 85 submitted applications for consideration.
- On June 1, 1998, opened the Center for Domestic Preparedness" at Fort McClellan, Alabama dedicated to training state and local emergency responders in both basic and advanced methods of responding to incidents of domestic terrorism. The Center, through its "live agent" training facility (the Chemical Defense Training Facility) offers advanced

training in the handling, management, and decontamination of incidents involving live chemical agents such as nerve agents and other toxins. Since opening on June 1, the Center has trained 550 First Responders in basic awareness, incident command, and incident management.

- In accordance with the FY 1998 Appropriations Conference Report language, a partnership has been formed with Texas A&M University, the Nevada Test Site, and the New Mexico Institute of Mining and Technology, as well as with the Louisiana State University and the OJP Center for Domestic Preparedness at Fort McClellan, to, through the combined assets of these entities, further assist state and local jurisdictions prepare for incidents of domestic terrorism. This partnership has been formalized by an agreement signed by all parties on June 11, 1998 which formally organized the "National Domestic Preparedness Consortium." The Consortium was formed to better coordinate the efforts of these individual entities and to maximize the use of their resources.
- On August 27th and 28th, 1998 convened a conference for state and local stakeholders which brought together over 200 state and local officials and representatives from the Federal government to discuss how the Federal government can best assist state and local jurisdictions respond to incidents of domestic terrorism. An executive Summary of the conferences significant findings and recommendations has already been produced and a full final report will soon be available.

OJP and OSLDPS are committed to working in partnership and cooperation with other Justice Department components, including the FBI, the Deputy Attorney General's Executive Office for National Security, the National Institute of Justice's Office of Science and Technology, and the Criminal Division's Antiterrorism and Violent Crime Section, as well as with other Federal agencies and departments, including FEMA, DOD, DOE and EPA, to ensure a coordinated Federal effort to assist state and local jurisdictions.

Office for State and Local Domestic Preparedness Support  
January 21, 1999

## BIOTERRORISM

### NEW ANNOUNCEMENTS

**New investment of \$11 million in Metropolitan Medical Response Teams.** Today, the President will announce a new, \$11 million investment in FY 1999 in new rapid medical response teams trained to respond to a biological or chemical weapons emergency. The Metropolitan Medical Response teams enhance local HAZMAT and emergency response systems by providing onsite victim extraction, antidote administration, decontamination, primary care, emergency medical transportation, and definitive, hospital based medical care and crisis counseling. This is an increase of almost 400 percent over their current FY 1999 funding level, and will support the development of teams in an additional 12 cities and takes a significant step towards the Administration's goal of establishing these teams in the 120 most densely populated metropolitan areas nationwide.

### PROGRAMS TO HIGHLIGHT

**Helping communities train emergency personnel about how to respond to bioterrorist attacks.** On March 15, 1999, the Department of Justice will award the first funds from their \$5 million competitive grant program designed to train State and local emergency response personnel (including firefighters) about how to respond to bioterrorist and other terrorist attacks. This program will conduct a community based needs assessment, develop training curricula, and delivery training both locally and at specialized training facilities. ~~They are scheduled to award the first training support funds on March 15, 1999.~~

**Helping communities purchase new equipment to protect emergency response personnel during a bioterrorist attack.** The Department of Justice is investing \$69.5 million in grants to States and municipalities to procure personal protective, chemical/biological agent detection, decontamination, and communications equipment to be used in the event of a bioterrorist attack. Of the \$69.5 million, approximately \$46 million will be awarded to the 157 largest cities and localities, with the amount based on population. The remaining \$24 million will be allocated to all 50 States, with a baseline amount of \$250,000 and the balance distributed on a population share basis.

Chris Jennings

Rm 216

**NATIONAL SECURITY COUNCIL**

January 7, 1999

Subject: **Anti-terrorism Event**

The NSC was asked to conceptualize a presidential event underscoring Administration efforts -- many of them new or enhanced with this budget -- to defend against terrorist threats.

Next Wednesday the 13<sup>th</sup>, was the original target date, but now that the 13<sup>th</sup> is spoken for, any date before release of the budget would do.

Such an event would deliver on the promises the President made in his Annapolis speech and roll out measures to combat "cyberterrorism" and to counter chemical and biological threats. A number of agencies -- HHS, DOJ, Commerce & others -- have a piece of the action.

The attached fact sheet & concept paper lay out our thinking. Comments welcome.

Thanks

*Alyn Davis*

X69461

January 13, 1999

## **Defending the United States from 21<sup>st</sup> Century Threats: Computer Attack and Chemical and Biological Weapons**

In his budget, President Clinton will propose a series of new programs that are vital to the defense of the homeland in this era of rapid technological change. These initiatives will build on two Presidential Decision Directives announced last May, which require the Federal Government to develop and implement new strategies on counterterrorism, weapons of mass destruction preparedness and critical infrastructure protection. In total, President Clinton will propose that the Federal Government spend \$9.6 billion to defend against terrorism, weapons of mass destruction and cyber attacks. This represents an increase of more than \$1.2 billion from the President's last budget proposal. Much of that money will be spent on the nontraditional threats that our nation will face in the 21<sup>st</sup> century.

**Cyber Terrorism.** Through cyber and other attacks on key computer systems, America could be brought to a standstill. The most critical sectors of our economy -- power-generation, telecommunications, banking, transportation and emergency services -- are all vulnerable to disruptions that would wreak havoc with the daily lives of our citizens. We know that other countries are developing capabilities for such disruption. To defend against a cyber attack, President Clinton will call in his forthcoming budget for path-breaking new programs to give the Federal Government the tools it needs to defend our communities and our economy from cyber terrorists and rogue states. In the first half of 1999, the President will unveil his National Plan for an unprecedented public-private partnership to protect these systems from cyber attack. In all, the President's budget will call for \$1.25 billion for critical infrastructure protection, up about \$200 million from the last fiscal year. New programs include:

~~\$400~~ —  
2

- **Cyber Corps:** Through this initiative, the United States can develop the experts we need to defend our critical infrastructure while giving students new opportunities to train themselves for high-skill, high-wage careers. College students who join will study computer science with tuition assistance for 5 years in return for a period of service in the Federal Government helping to safeguard computers at agencies such as Social Security, FAA and FEMA. The program will both alleviate the Federal Government's difficulty in recruiting computer experts and create incentives for colleges to offer more advanced courses in computer science. Modeled on the ROTC, Cyber Corps will be established in FY00 and the first scholarships granted in FY01.
- **Computer Intrusion Detection Networks:** This initiative will make a vital difference in protecting the systems that keep government running, thus safeguarding our national security and daily economic life. Monitors on each critical computer system will be networked together so that when one computer system is attacked the network will instantly inform all other critical government systems of the source of the intrusion, the mode of attack and how to stop it. The Department of Defense has initiated work on a similar system; we will commence work on a civilian agency network in FY00. The two government networks will provide a model for private sector critical infrastructure efforts in industries such as banking, electricity, and transportation.

- **Information Sharing and Analysis Centers:** As part of the Public-Private Partnership, Federal agencies will support the initial establishment of ISACs to foster private sector development of best practices and standards, the sharing of threat analysis, foster discussion of best defensive measures, and provide outreach and training programs. These ISACs will enable fuller exchange of information between the private sector and the National Infrastructure Protection Center, established last year at the FBI, without compromising on privacy or civil liberties.
- **Computer Security Applied Research Initiative:** This effort will focus on methods of improving information assurance by safeguarding networks and data bases. Part of the initiative will focus on developing artificial intelligence that can identify anomalous activities as well as "trap doors," "Trojan horses," and other malicious code installed by unauthorized users. Because computer software is being widely rewritten for Y2K, there is now heightened concern about the covert installation of unauthorized code.

**Biological and Chemical Terrorism.** As technology advances, the means of developing weapons of mass destruction are increasingly accessible for terrorists and rogue states. In the wake of the sarin gas attack in the Tokyo subway, we know that the threat is real -- and that we must work to prevent such an attack from happening and be ready to respond if one should occur. President Clinton's budget expands efforts underway to increase the safety of American citizens from these terrible weapons by increasing funding by more than \$100 million. These funds will help pay for:

- 30
- **Vaccine Research and Development:** With last year's budget supplemental, President Clinton began funding for the nation's first civilian medical stockpile, which will provide necessary medicines, antidotes and vaccines in case of biological or chemical attack. Ensuring that we have the right medicines means not only buying ones currently in production but also developing new ones for diseases that are virtually never seen. The President's budget will fund research and development for vital vaccines for which there is currently little or no market though they are needed to protect against some of the most fearsome biological weapons agents.
  - **Public Health Surveillance:** Unlike other kinds of attack, a biological weapons release could go undetected for days or longer. Stopping the spread of a disease and treating those at risk of contracting the illness requires that the pathogen is identified quickly. To achieve that rapid response, our public health system must be upgraded so doctors and other medical workers can recognize outbreaks of diseases caused by biological agents. The President's budget will fund necessary improvements in laboratories, training and data bases so that our experts have the essential tools they need to sound the alarm when a biological attack has occurred and start the necessary work to treat the sick and halt the spread of infection.
  - **National Assets:** To assist local emergency management, personnel will be enhanced where they exist and established where they are lacking. These assets will include elements from the National Guard, Army, Marines and Coast Guard.
  - **National Domestic Preparedness Office:** This office was established in November and will help create a national contingency plan for 120 metropolitan areas and provide a single, integrated federal program to train and equip the first responder community across the country in biological, chemical, and nuclear weapons of mass destruction preparedness.
- not this

DRAFT

DATE: ~~January 12, 1999~~  
LOCATION: East Room  
TIME: TBD

I. PURPOSE

To announce new programs in the President's FY 2000 budget to defend the United States from cyber terrorism and chemical and biological terrorism.

II. BACKGROUND

Last May POTUS announced two Presidential Decision Directives which required the Administration to develop new strategies on counterterrorism, weapons of mass destruction preparedness and critical infrastructure protection. In his FY 2000 budget, POTUS will propose increased funding for these initiatives to a total of \$9.6 billion -- \$1.2 billion more than POTUS's last budget proposal. Much of that money will be spent on new programs to combat nontraditional, 21<sup>st</sup> century threats. These threats include cyber terrorism (such as the Solar Sunrise attack on Pentagon computers) against the most critical sectors of our economy such as power-generation, telecommunications, banking, transportation and emergency services. Funding for new programs to defend against cyber terrorism will increase by about \$200 million. POTUS will also propose an increase of about \$100 million for new programs to defend against chemical and biological terrorism such as the sarin gas attack in the Tokyo subway. New programs include cyber corps, detection nets, and public health surveillance (see fact sheet).

III. PARTICIPANTS

Speaking roles: POTUS, VPOTUS, Sam Nunn, Josh Lederberg, Alfred Berkeley (or Chuck Lee). Standing behind podium: Reno, Shalala, Daley, Berger, Clarke

IV. SEQUENCE (Total POTUS time: 50 minutes)

- |                                                                  |            |
|------------------------------------------------------------------|------------|
| 1. POTUS/VPOTUS briefing time w/Berger and Clarke                | 15 minutes |
| 2. VPOTUS introductory remarks                                   | 3 minutes  |
| 3. Sam Nunn remarks on growing unconventional threats            | 5 minutes  |
| 4. Alfred Berkeley (or Chuck Lee) remarks on cyber terror threat | 5 minutes  |
| 5. Josh Lederberg remarks on chem/bio terror threat              | 5 minutes  |
| 6. POTUS remarks                                                 | 10 minutes |
| 7. POTUS works the room                                          | 5 minutes  |
| 8. POTUS departs & validators meet w/press                       |            |

V. PRESS PLAN

After POTUS event, briefing in WH Press Room: Reno, Shalala, Daley, Clarke.  
Interviews scheduled for selected cyber terrorism validators (Nunn, Berkeley, Lee, Gorelick, Augustine) and chem/bio terrorism validators (Lederberg, Young, Hauer,)

DRAFT

VI. POTENTIAL INVITEESCyber Terrorism

| NAME                       | TITLE                | CO. / ORG                                     | REASON   |
|----------------------------|----------------------|-----------------------------------------------|----------|
| Lee, Charles               | Chairman and CEO     | GTE Corp.                                     | Adv Comm |
| Mineta, Norman             | VP                   | Lockheed Martin                               | Adv Comm |
| Ellsworth, Bob             |                      |                                               |          |
| Berkeley, Alfred           | President            | NASDAQ                                        |          |
| Augustine, Norm            |                      |                                               |          |
| Gorelick, Jamie            | Vice Chairman        | Fannie Mae                                    | Adv Comm |
| Nunn, The Honorable Sam    | Partner              | King and Spalding                             | Adv Comm |
| Moon, Elvin                | President            | EW Moon Engineering and Const Mgmt Industries | Adv Comm |
| Adams, James               | CEO                  | I-Defense                                     | Author   |
| Nye, Erle                  | Chairman and CEO     | Texas Utilities Company                       | Adv Comm |
| Greenburg, Maurice         | Chairman and CEO     | American International Group                  | Adv Comm |
| Greene, Margaret           | VP and Gen Counsel   | BellSouth Corporation                         | Adv Comm |
| Holmes, Joseph             | VP                   | EDS                                           | Adv Comm |
| Jaffe, Dr. Jeffrey         | VP of Technology     | IBM Corporation                               | Adv Comm |
| Baxter, Bob                | President            | Bechtel Civil Company                         | Adv Comm |
| Berdahl, Robert            | Chancellor           | Univ of California, Berkeley                  | Adv Comm |
| Campbell, David            | President and CEO    | BBN Technologies                              | Adv Comm |
| Davis, Jerome              | President and CEO    | NoxTech                                       | Adv Comm |
| Fisher, Richard            | Chairman             | Morgan Stanley Group                          | Adv Comm |
| Sayles Belton, Sharon      | Mayor of Minneapolis |                                               | Adv Comm |
| Topfer, Mort               | Vice Chairman        | Dell Computers                                | Adv Comm |
| Wicks, Floyd               | President            | Southern California Water Company             | Adv Comm |
| Banker, Elizabeth          |                      | Steptoe and Johnson, LLP                      | PCCIP    |
| Culnan, Mary J.            | Professor            | Georgetown University                         | PCCIP    |
| Keyes, David               | Senior Manager       | KPMG                                          | PCCIP    |
| Kurtz, James               |                      | Institute for Defense Analysis                | PCCIP    |
| Lacombe, Phil              |                      | Veridian                                      | PCCIP    |
| Marsh, Tom                 | General              | Air Force Aid Society                         | PCCIP    |
| Reynolds, Charles          | Interim Dean         | James Madison University                      |          |
| Schumann, Larry J.         | President and CEO    | NTA                                           | NSTAC    |
| Chilcoat, Lt. Gen. Richard | President            | National Defense University                   |          |
| Leffler, L. G.             | NERC Project Manager | NERC                                          |          |
| Jones, Anita K.            | Professor            | University of Virginia                        |          |
| Wulf, William A.           | President            | National Academy of Engineering               |          |

|                         |                                              |                                             |       |
|-------------------------|----------------------------------------------|---------------------------------------------|-------|
| Spillman, Larry D.      | VP                                           | AT&T                                        |       |
| Holleyman, Robert W.    | President and CEO                            | Business Software Alliance                  |       |
| Allen, Catherine        | Banking Industry Technologies Secretariat    | Bankers Roundtable                          |       |
| Katz, Stephen           | VP and Chief Information Security Officer    | Citibank                                    |       |
| Massa, James            | Director, Government Alliances               | Cisco Systems                               |       |
| Wallace, Ernest         | Director, Nat Sec'y Relations                | COMSAT                                      |       |
| Silliman, Scott         | Executive Director                           | Duke University School of Law               |       |
| Goodman, Sy             | Professor                                    | Stanford University                         |       |
| Roth, Kevin             | Program Manager                              | ITAA                                        |       |
| Geiger, William H.      | President and CEO                            | Aegis Research Corporation                  |       |
| Alberthal, Lester M.    | Chairman and CEO                             | EDS                                         | NSTAC |
| Peerenboom, Dr. James   | Director, Infrastructure Assurance Center    | Argonne National Laboratory, U of C         |       |
| Ware, Willis H.         | Chairman, Research Staff                     | Rand                                        |       |
| Sanovic, Randolph       | Gen Director, Info Security                  | General Motors Corporation                  |       |
| Vetter, Linda           |                                              | Agorics, Inc.                               |       |
| Wade, James R.          | Director, Fraud and Enterprise Info Security | Airtouch Cellular                           |       |
| Littlejohn, Gail        | Senior VP                                    | Lexis-Nexis Corporation                     |       |
| Jacobson, Jennifer      | Public Policy Counsel                        | America Online                              |       |
| McConnell, Mike         | VP                                           | Booz Allen and Hamilton                     | NSA   |
| Schlosser, Lynn         | Director, Federal Affairs                    | Eastman Chemical Company                    |       |
| Copeland, Guy           | VP, Information Infrastructure               | CSC                                         | NSTAC |
| Allen, Julia            | Software Eng. Institute                      | Carnegie Mellon University                  |       |
| Van Voorhies, Robert F. |                                              | Bryan Cave LLP                              |       |
| Rindskopf, Elizabeth    | Crit Infra Assur Counsel                     | American Bar Association                    |       |
| Oettinger, Anthony      | Professor                                    | Harvard University                          |       |
| Ackerman, F. Duane      | President and CEO                            | BellSouth Corporation                       |       |
| Armstrong, Michael      |                                              | AT&T                                        |       |
| Babbio, Lawrence T.     | Pres. and CEO, Network Group                 | Bell Atlantic Corporation                   |       |
| Ballmer, Stephen        | Executive VP, Sales & Support                | Microsoft Corporation                       |       |
| Black, Edward           | President                                    | Computer and Communications Industry Assoc. |       |

|                      |                                                |                                                       |       |
|----------------------|------------------------------------------------|-------------------------------------------------------|-------|
| Chase, Steve         | President and CEO                              | America Online                                        |       |
| Cahouet, Frank V.    | President and CEO                              | Mellon Bank and Mellon Bank Corp.                     |       |
| Cerf, Vinton G.      | Senior VP                                      | MCI Communications Corp.                              |       |
| Dawson, Rhett B.     | President                                      | Information Technology Industry Council               |       |
| Duques, Henry C.     | CEO                                            | First Data Corporation                                |       |
| Flanigan, Matthew J. | President                                      | TIA                                                   |       |
| Gerstner, Louis V.   | CEO                                            | IBM Corporation                                       |       |
| Hewitt, Charles      | President                                      | Satellite Broadcasting and Communications Association |       |
| Kuhn, Tom            | President                                      | Edison Electric Institute                             |       |
| Lutnick, Howard      | President and CEO                              | Cantor Fitzgerald                                     |       |
| McColl, Hugh         | CEO                                            | Nationsbank                                           |       |
| McCaw, Craig         | CEO                                            | Teledesic Corp.                                       |       |
| McGinn, Richard      | President and CEO                              | Lucent Technologies Inc.                              |       |
| McNealy, Scott       | President and CEO                              | Sun Microsystems                                      |       |
| Miller, Harris       | President                                      | Information Technology Association of America         |       |
| Moore, Gordon        | Chairman Emeritus                              | Intel Corporation                                     |       |
| Chambers, John       | President and CEO                              | Cisco Systems                                         |       |
| Eisenberg, Lewis     | Chairman of Port Authority, NY and NJ          |                                                       |       |
| Platt, Lewis E.      | President and CEO                              | Hewlett Packard Company                               |       |
| Reed, John S.        | Chairman and CEO                               | CITICORP                                              |       |
| Tooker, Gary         | Chairman                                       | Motorola Inc.                                         |       |
| Viterbi, Andrew      | Vice Chairman                                  | Qualcomm, Inc.                                        |       |
| Wheeler, Thomas      | President and CEO                              | Cellular Telephone Industry Association               |       |
| Winkler, Michael     | Senior VP and Group General Manager            | COMPAQ                                                |       |
| Yeager, Curt         |                                                | Electric Power Research Institute                     |       |
| Zarb, Frank          | Chairman and CEO                               | National Association of Securities Dealers, Inc.      |       |
| Hilsman, William J.  | Chairman of the Board                          | Advanced Digital Technologies Company                 | NSTAC |
| Stroebele, John A.   | President                                      | Advanced Digital Technologies Company                 | IES   |
| Stein, Martin A.     | Vice Chairman, Automation and Support Services | BankAmerica Corporation                               | NSTAC |
| Cheng, George        | Senior VP                                      | BankAmerica Corporation                               | IES   |
| Evatt, James W.      | President, Information and Communications      | The Boeing Company                                    |       |

|                        |                                                          |               |
|------------------------|----------------------------------------------------------|---------------|
|                        | Preparedness                                             |               |
| Dr Tony Fauci          | HHS, Institute for Allergies and Infectious Diseases     | Director      |
| Ms Sarah Layton        | American Public Works Association                        | Director      |
| Mr Raymond Sheppach    | National Governor's Association                          | Exec Director |
| Mr Carl Tubbesing      | National Conference of State Legislators                 | Director      |
| Mr Larry Naake         | National Association of Counties                         | Exec Director |
| Mr J. Thomas Cochran   | National Conference of Mayors                            | Exec Director |
| Mr Donald Borut        | National League of Cities                                | Exec Director |
| Mr William Hansell     | International City Managers Association                  | Exec Director |
| Mr Tom Halicki         | National Association of Towns and Townships              | Exec Director |
| Mr Garry Briese        | International Association of Fire Chiefs                 | Exec Director |
| Mr Alfred Whitehead    | International Association of Fire Fighters               | President     |
| Mr Fred Allinson       | National Volunteer Fire Council                          | Chairman      |
| Mr Romeo Spaulding     | International Society of Fire Service Inspectors         | Exec Director |
| Mr Alan Walker         | National Association of State Fire Training Directors    | President     |
| Mr William Webb        | Congressional Fire Services Institute                    | Exec Director |
| Mr Dan Rosenblatt      | International Association of Police Chiefs               | Exec Director |
| Mr A.N. Moser          | National Sheriffs Association                            | Exec Director |
| Mr Chuck Wexler        | Police Executive Research Forum                          | Exec Director |
| Mr Hubert Williams     | Police Foundation                                        | President     |
| Mr Robert Stewart      | National Association of Black Law Enforcement Executives | Exec Director |
| Mr Rick Murray         | American College of Emergency Physicians                 | EMS Manager   |
| Ms Trina Hembree       | National Emergency Management Association                | Exec Director |
| Ms Elizabeth Armstrong | International Association of Emergency Managers          | Exec Director |

#### Members of Congress

- To be provided by White House and NSC Legislative Affairs

*Jessica being writer*

|                     |                                                                 |                                                    |
|---------------------|-----------------------------------------------------------------|----------------------------------------------------|
| Steele, Robert W.   | Systems<br>General Manager,<br>Business Development<br>Planning | Boeing Information<br>Services                     |
| Parker, David       | President                                                       | American Gas Association                           |
| Richardson, Alan H. | Executive Director                                              | American Public Power<br>Association               |
| English, Glen       | CEO                                                             | National Rural Electric<br>Cooperative Association |
| Lee, William C.Y.   | VP and Chief Scientist                                          | Air Touch Communications                           |
| Bishop, William     | President                                                       | Institute of Internal Auditors                     |
| Burnett, William    | Senior VP                                                       | Gas Research Institute                             |
| Grimes, John        | VP                                                              | Raytheon E-Systems                                 |
| Hahn, Richard       | VP                                                              | Boston Edison                                      |
| Hoffman, Lance J.   | Professor                                                       | George Washington<br>University                    |
| Blatt, William J.   | VP                                                              | Northern Telecom                                   |
| Blumentfeld, Seth   | President and COO                                               | MCI International                                  |
| Burk, Arthur        | Senior Safety Fellow                                            | DuPont Excellence Center                           |
| Rotenberg, Mark     | Executive Director                                              | Electronic Privacy<br>Information Center           |
| Berman, Jerry       | Executive Director                                              | Center for Democracy and<br>Technology             |
| Neal, Roy           | President and CEO                                               | US Telephone Association                           |
| Goodman, Seymour    | Center for International<br>Security and Arms<br>Control        | Stanford University                                |
| Foster, Joe         | Chairman                                                        | National Petroleum Council                         |

#### Chemical/Biological Terrorism

|                     |                                      |                                            |
|---------------------|--------------------------------------|--------------------------------------------|
| Mr Louis Freeh      | FBI                                  | Director                                   |
| Mr Tom Kuker        | National Defense Preparedness Office | Director                                   |
| Mr Frank Young      | Reformed Theological Seminary        | Fmr Director, FDA                          |
| Mr Jerry Houer      | NYC                                  |                                            |
| Dr Josh Lederberg   | Rockefeller University               | Nobel Laureate                             |
| Mr                  | OSD-Reserve Affairs                  |                                            |
| Dr Margaret Hamburg | HHS                                  | Asst Sec'y for<br>Policy, Plng and<br>Eval |
| Dr David Satcher    | HHS                                  | Surgeon General                            |
| Dr William Raub     | HHS                                  | DAS for Policy                             |
| Dr James Hughes     | CDC                                  | Director for<br>Infectious Diseases        |
| Dr Bob Knouss       | HHS, Office of Emergency             | Director                                   |

|                        |                                                          |               |
|------------------------|----------------------------------------------------------|---------------|
|                        | Preparedness                                             |               |
| Dr Tony Fauci          | HHS, Institute for Allergies and Infectious Diseases     | Director      |
| Ms Sarah Layton        | American Public Works Association                        | Director      |
| Mr Raymond Sheppach    | National Governor's Association                          | Exec Director |
| Mr Carl Tubbesing      | National Conference of State Legislators                 | Director      |
| Mr Larry Naake         | National Association of Counties                         | Exec Director |
| Mr J. Thomas Cochran   | National Conference of Mayors                            | Exec Director |
| Mr Donald Borut        | National League of Cities                                | Exec Director |
| Mr William Hansell     | International City Managers Association                  | Exec Director |
| Mr Tom Halicki         | National Association of Towns and Townships              | Exec Director |
| Mr Garry Briese        | International Association of Fire Chiefs                 | Exec Director |
| Mr Alfred Whitehead    | International Association of Fire Fighters               | President     |
| Mr Fred Allinson       | National Volunteer Fire Council                          | Chairman      |
| Mr Romeo Spaulding     | International Society of Fire Service Inspectors         | Exec Director |
| Mr Alan Walker         | National Association of State Fire Training Directors    | President     |
| Mr William Webb        | Congressional Fire Services Institute                    | Exec Director |
| Mr Dan Rosenblatt      | International Association of Police Chiefs               | Exec Director |
| Mr A.N. Moser          | National Sheriffs Association                            | Exec Director |
| Mr Chuck Wexler        | Police Executive Research Forum                          | Exec Director |
| Mr Hubert Williams     | Police Foundation                                        | President     |
| Mr Robert Stewart      | National Association of Black Law Enforcement Executives | Exec Director |
| Mr Rick Murray         | American College of Emergency Physicians                 | EMS Manager   |
| Ms Trina Hembree       | National Emergency Management Association                | Exec Director |
| Ms Elizabeth Armstrong | International Association of Emergency Managers          | Exec Director |

#### Members of Congress

- To be provided by White House and NSC Legislative Affairs

## Infrastructure

- MMRs
- research & development
- deterrents

**P R I O R I T Y   H A N D L I N G****N A T I O N A L   S E C U R I T Y   C O U N C I L****F A X   C O V E R   S H E E T****NATIONAL  
SECURITY  
COUNCIL****17th & Penn, N.W.  
Washington, D.C.  
20504****Did you get a complete,  
clear transmission? If not,  
please call:  
CAROLYN DOLLAR  
(202) 456-9361****From: DANIEL BENJAMIN****To: DEVORAH ADLER****Agency: ODP****Fax Number: 6-5557****Date/Time: 1/21/99 3:00 PM****No. of pages to follow: 2****Message: BW FACT SHEET IS BEING  
FORWARDED PER YOUR TELCON WITH DAN  
BENJAMIN. THANK YOU. CAROLYN DOLLAR**

# Withdrawal/Redaction Marker

## Clinton Library

| DOCUMENT NO.<br>AND TYPE | SUBJECT/TITLE                                                                                | DATE       | RESTRICTION      |
|--------------------------|----------------------------------------------------------------------------------------------|------------|------------------|
| 002. paper               | re: President Clinton's Initiative on Biological and Chemical Weapons Preparedness (2 pages) | 01/21/1999 | b(7)(E), b(7)(F) |

### COLLECTION:

Clinton Presidential Records  
Domestic Policy Council  
Devorah Adler  
OA/Box Number: 20146

### FOLDER TITLE:

Bioterrorism [Folder 4]

2012-0463-S

rc693

### RESTRICTION CODES

#### Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]  
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]  
P3 Release would violate a Federal statute [(a)(3) of the PRA]  
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]  
P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [(a)(5) of the PRA]  
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

C. Closed in accordance with restrictions contained in donor's deed of gift.

PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).

RR. Document will be reviewed upon request.

#### Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]  
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]  
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]  
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]  
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]  
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]  
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]  
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

## Bioterrorism

POTUS

VP

500 people?

## Venue

Natl Academy of Sciences

Police Dept

Fire Dept housing

prototype for vehicle  
for chem-bio response

"Keeping America Secure"?

DOS

HHS

DOD

} participating  
agencies

OPM

OFA

## Audience

ass heads

academic

local police etc

invites for Tuesday

Shalala speaking? ♀  
as opposed to ♂

list of agency invites -  
David B.

President NYT interview  
Th → F journalists

Cabinet members @ top of  
Joe's briefing

fact sheets, etc.

BN \$100

cyber \$400

Another Russian scientist said that during a visit to Teheran last year he had encountered three former colleagues from the Institute of Biological Protection in Moldova who had already been in Teheran for about six months.

"They told me their institute had neither heat nor electricity, never mind money for salaries or research," the scientist recalled. "Russian scientists may not trust or like Iranians," he added. "But these are not love matches. They are marriages of convenience, and often of necessity."

## The Prize

# Deadly Appeal Of an Ex-Arsenal

It is now known that the Soviet Union built the most pestilential germ arsenal of all time. At the peak of Soviet activity, Russian and Western experts say, germ scientists at scores of sites studied some 50 agents and prepared a dozen or so for war. Bombers and intercontinental missiles were ready to disseminate hundreds of tons of smallpox, plague and anthrax, enough to wipe out entire nations.

Many of these biological agents were developed and tested at several sites: the State Research Center of Virology and Biotechnology, known as Vector, which made deadly viruses in Siberia; the State Research Center for Applied Microbiology, at Obolensk,

near Moscow, where tetanar bacteria were perfected, and Stepnogorsk, the germ factory in Kazakhstan, which specialized in deadly anthrax.

This proud elite was part of a culture with a history of deeply distrusting Islamic regimes, which threatened to undermine the Soviet empire. Thus, any current Iranian successes are all the more striking.

Since the collapse of Soviet Communism, these scientific centers, as well as far smaller ones, have seen their operating budgets slashed and research money disappear. But institute directors say they have fought to keep their top talent intact, dismissing junior scientists and technical workers instead.

Yet even high-level scientists have been tempted to sell their expertise.

Igor Domaradskij, a founder of the main Soviet program to make germ weapons, lives in a spacious apartment in a fashionable part of Moscow, a reminder of the privileges and status he once enjoyed as director of the antiplague institutes in Irkutsk and Rostov-on-Don and later as a key figure at Obolensk.

His doorbell now consists of two wires that must be twisted together to create a ring, and his preoccupation with making a living is a theme of "The Troublemaker," his memoir of his years as a germ scientist.

Dr. Domaradskij, 73, says he lives off his pension and his savings. And he is fortunate in having a computer and E-mail that connect him to scientists outside Russia. But he disclosed in his book that he was so desperate for work in 1992 that he offered his services to China, Russia's longtime rival, as well as to the Kalmyk Republic inside Russia. Neither responded, he said.

Russia's economic chaos, which worsened in August with the collapse of the ruble, has taken a huge toll on nearly all of the scientific organizations once lavishly funded by the germ bureaucracy.

Obolensk, once one of the top centers, lost 54 percent of its staff between 1990 and 1996 but only 28 percent of its top scientists, according to the institute's figures.

That exodus is understandable given the stark working conditions. At institute after institute, there are empty rooms; for months on end there has been no pay and scant heat for scientists trying to work wrapped in layers of sweaters. Prospects thus seem better almost anywhere else.

"Like everyone else, we're just trying to survive," said Yevgeny A. Nepoklonov, 42, director of Narvac, an animal vaccine company that employs some 50 scientists, many from the former weapons program.

Narvac, with \$3 million in total sales, is testing a vaccine against hog cholera that would be Russia's first genetically engineered animal vaccine. The laboratory has great hopes for the product, if it can survive Russia's economic turmoil.

The Russian Government has sent mixed signals about the Iranian overtures.

In May of 1997, Moscow went so far as to sponsor a biotechnology trade fair in Teheran. Participants included more than 100 leading biologists from Russian laboratories once part of the germ warfare program, including Vector and Obolensk, the two most prominent sites.

And President Boris Yeltsin has kept in senior civilian biotechnology posts several key military figures from the old Soviet germ program, some of whom are openly hostile to the growing cooperation between American and Russian scientists.

Moscow has embraced the Clinton Administration's programs to forge closer scientific ties even as it allows some institutes to strike commercial deals with Iran.

Vector, for example, has been permitted to sell Iran diagnostic kits for hepatitis. But the institute has refused Iranian requests for broader technological cooperation or the exchange of dangerous strains, according to American officials and Dr. Sandakhchiev, Vector's chief.

"There is a very fine line between good and bad dealings," he said, "which is why I am concerned about the challenge of bioterrorism."

TUESDAY, DECEMBER 8, 1998

# Dollars Are Weapon of Choice in the War on Bacteria Peril

By JUDITH MILLER  
with WILLIAM J. BROAD

MOSCOW — In Russia's scientific despair, the United States has sensed great danger and opportunity.

American officials have been worried about Russia's weapons programs from the moment the Soviet Union collapsed in 1991. Initially, the focus was on improving security for nuclear weapons and scientists. The germ warfare program was hardly considered.

That changed after several top Soviet germ warriors defected to the West and told intelligence officials that Moscow's germ program was far more lethal and ambitious than had been suspected during the cold war.

At the Pentagon's request and with its money, the National Academy of Sciences began a program in 1995 to expand cooperation between Russian and American biologists. Eager to stem the brain drain, discover more about the Soviet germ arsenal, and learn from the Russian strides in germ defenses, the Clinton Administration has now greatly intensified the effort.

In addition, Washington is paying \$1.5 million now and plans to spend up to \$6 million to upgrade security at Vector, which is Russia's germ bank for all strains of smallpox, which has been eradicated from humans.

While fewer than 120 of the more than 15,000 strains in Vector's virus collection are highly lethal, scientists say any theft or diversion of the most dangerous ones could be catastrophic.

Washington has also persuaded Europe and Japan to join the United States in financing the International Sci-

## U.S. is said to be spending millions in making 'a better offer' to Russian scientists.

ence and Technology Center, based in Moscow, which tries to find peaceful work for former weapons scientists.

Randall L. Beatty, the center's deputy director, said about 1,055 of the 17,800 scientists receiving payments of \$300 to \$500 a month for joint research are biologists. That proportion has grown sharply from less than 1 percent of the center's payments to about 15 percent this year, and Mr. Beatty said it "will inevitably grow further."

While less than what the Iranians are said to be offering, American officials say the stipends are attractive because they allow Russian scientists, who earn an average of less than \$100 a month, to stay in Russia with friends and family and to collaborate with respected Western researchers on peaceful work.

American officials said such contacts and exchanges are providing valuable information about both the Soviet Union's germ activities and the current situation in Russia. "There has been a quantum leap in their openness in the past 18 months," Mr. Beatty said.

The Clinton Administration is spending millions of dollars on more than a dozen programs essentially intend-

ed to make former Soviet scientists and research institutes "a better offer" than Iran or other rogue nations, official say.

"It's up to them to chose," said Anne M. Harrington, the State Department's coordinator for threat reduction programs, "and many of them are deciding they want to work with us."

American officials say the rudimentary programs have already achieved some successes.

¶The scientific institute at Obolensk, the heart of the program to produce deadly germs, has had no contact with Teheran since last year when the United States greatly expanded its financial support.

¶In the last 10 months close to a hundred Russian scientists from the former Soviet germ warfare program have visited American labs and institutes, and more than a hundred American scientists and officials have visited, many of them regularly, once-closed Russian germ institutes.

¶The Department of Agriculture, at the Pentagon's request, succeeded in buying samples of Uzbekistan's entire collection of plant germs, helping to track strains and create antidotes.

American officials say that the threat remains significant, and that they are learning every day about new efforts by rogue states to capitalize on Russia's economic crisis and scientific brain drain.

"I'm like the little Dutch boy running around with my fingers in the dike," said a Pentagon official during a recent field trip. "Every time we visit a new Russian institute, we find another Iranian business card."

NATIONAL SECURITY COUNCIL  
WASHINGTON, D.C. 20504

WW  
0279

January 16, 1999

ACTION

MEMORANDUM FOR SAMUEL R. BERGER

FROM: RICHARD A. CLARKE *RA Clarke*  
SUBJECT: POTUS NYT Interview on Bioterrorism

Attached for your signature is a meeting memo for the President regarding his interview on Thursday, January 21, with Judy Miller and William Broad of the New York Times.

Concurrence by: David Leavy, Elisa Harris, Ken Bernard *ELH*

RECOMMENDATION

That you sign the attached memorandum for the President.

Attachments

Tab I Memorandum for the President  
Tab A Talking Points for Opening Remarks  
Tab B Questions and Answers  
Tab C Recent Related Articles by Miller and Broad

# Withdrawal/Redaction Marker

## Clinton Library

| DOCUMENT NO.<br>AND TYPE | SUBJECT/TITLE                                                                  | DATE       | RESTRICTION |
|--------------------------|--------------------------------------------------------------------------------|------------|-------------|
| 003a. memo               | From: Samuel Berger re: Interview with Judy Miller and William Broad (5 pages) | 01/21/1999 | P1/b(1)     |

### COLLECTION:

Clinton Presidential Records  
Domestic Policy Council  
Devorah Adler  
OA/Box Number: 20146

### FOLDER TITLE:

Bioterrorism [Folder 4]

2012-0463-S

rc693

### RESTRICTION CODES

#### Presidential Records Act - [44 U.S.C. 2204(a)]

- P1 National Security Classified Information [(a)(1) of the PRA]
- P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
- P3 Release would violate a Federal statute [(a)(3) of the PRA]
- P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
- P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [(a)(5) of the PRA]
- P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

C. Closed in accordance with restrictions contained in donor's deed of gift.

PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).

RR. Document will be reviewed upon request.

#### Freedom of Information Act - [5 U.S.C. 552(b)]

- b(1) National security classified information [(b)(1) of the FOIA]
- b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
- b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
- b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
- b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
- b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
- b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
- b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

A

# Withdrawal/Redaction Marker

## Clinton Library

| DOCUMENT NO.<br>AND TYPE | SUBJECT/TITLE                                              | DATE | RESTRICTION |
|--------------------------|------------------------------------------------------------|------|-------------|
| 003b. talking<br>points  | re: Interview with Judy Miller and William Broad (2 pages) | n.d. | P1/b(1)     |

### COLLECTION:

Clinton Presidential Records  
Domestic Policy Council  
Devorah Adler  
OA/Box Number: 20146

### FOLDER TITLE:

Bioterrorism [Folder 4]

2012-0463-S  
rc693

### RESTRICTION CODES

#### Presidential Records Act - [44 U.S.C. 2204(a)]

- P1 National Security Classified Information [(a)(1) of the PRA]
- P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
- P3 Release would violate a Federal statute [(a)(3) of the PRA]
- P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
- P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [(a)(5) of the PRA]
- P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

C. Closed in accordance with restrictions contained in donor's deed of gift.

PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).

RR. Document will be reviewed upon request.

#### Freedom of Information Act - [5 U.S.C. 552(b)]

- b(1) National security classified information [(b)(1) of the FOIA]
- b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
- b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
- b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
- b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
- b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
- b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
- b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

**B**

## **BIOTERRORISM Q&A**

**We've heard a great deal about this – Cohen has warned of the a five pound bag of anthrax, novelists spin tales of bio-engineered Ebola virus, bin Ladin is reported to be searching for biological weapons. What worries you most?**

- One challenge is my responsibility to inform the American people about a threat to their interests without unduly alarming them or tipping off our enemies. Three part strategy: deterrence by ensuring that we have the capacity and will to take action against those who may attack us using CBW, preventive action against those irrational actors who might not be deterred, and preparedness to deal with an attack should one occur despite our best efforts.
- Rouge states and terrorists interested in CBW. If we knew about a specific immediate threat to use CBW, we would deal with it directly.
- That's why I directed a major new defensive program: building a civilian medical stockpile; researching new vaccines and medicines; upgrading our national public health surveillance and laboratory system to detect BW; having emergency response people trained and ready. Good start to a long-term project. This year I will ask for \$1.3 billion for this overall effort.
- Law enforcement is critical. Since the I came into office, I have raised the FBI's counter-terrorism budget by 283%, from \$78m in FY93 to \$301m in FY99. (As a percentage of the overall FBI budget, C/T has risen from 4% to 10%.) FBI agents assigned to C/T have risen from 550 to 1383 (from 5% of agents to 12% of agents).

**But let's say that Secretary Cohen's bag of anthrax was sprayed over downtown Washington or a comparable amount of smallpox virus was released. What could we do?**

- I don't think horror scenarios are going to help us. It won't do us any good for people to panic or for us to write a prescription for an enemy's attack.
- Better to focus on preparedness. One of the best strategies for deterring a BW attack is to ensure such an attack would cause little harm. That robs the terrorist of the shock value they are looking for. That's why we are increasing preparedness now.

**Is Usama bin Ladin is developing chemical or biological weapons. What are we doing?**

- He has a longstanding interest in developing WMD and he has spoken about his willingness to use such weapons against us. I won't go into intelligence matters, but I can assure you that we have not let up for a moment in our efforts to stop bin Ladin.

**What if Iran got its hands on a genetic mutant agent, such as merging Ebola and smallpox. Couldn't we face a plague from something that we had not developed a medicine against?**

- This is why we need to have an active research effort that could quickly analyze a new threat and move rapidly into production of a new medicine. That is why we are increasing R&D.

**What are you doing about all these anthrax hoaxes we've heard about recently?**

Strengthening law enforcement. Two people in California have already been arrested.

**Critics have said we need a Homeland Defense Command or a Cyberspace Command, a real Czar. Why not?**

- Sometimes rapid evolutionary change in government produces better results than disruptive revolutionary change. We will be making changes in the military structure later this year to better address Homeland Defense and Cyberspace Defense.
- Many changes in the bureaucracy already: National Coordinator in the White House with real clout, an interagency National Domestic Preparedness Office, an interagency National Infrastructure Protection Center, a DOD Joint Task Force for Cyber Defense.

**Why have the health consequences of terrorism not been emphasized until recently?**

- Actually we've been systematically emphasizing the health consequences of biological or chemical terrorism since we first began preparing for the 1996 Olympic Games in Atlanta. Congress has agreed with my emphasis on strengthening the public health infrastructure, particularly at the community level.

**Where does the stockpile project stand now and what should be in it? What do you mean by a "stockpile"? What will be in the stockpile?**

- Funds just became available from the Congress in October, so we're in the beginning phase. This year we will buy medicines currently in production. Also investing \$30 million more in R&D this year to develop the new vaccines and medicines we will need.
- Assuring rapid access to enough drugs and vaccines after an attack. That means helping ensure drug companies have sufficient inventories, helping communities purchase these antidotes, and making sure drugs can be rapidly taken where they are needed and distributed.
- Initial focus on treating anthrax, plague, and tularemia. We will enhance the usefulness of our current supply of smallpox vaccine and will develop a cache of drugs and equipment for countering chemical attacks. R&D will work on antiviral drugs for anthrax and smallpox.

**The World Health Assembly has called for the destruction in June of the last remaining stores of smallpox now being held in Russia and the U.S. U.S. opposes. Why are you worried about treatments and diagnosis if all the virus is destroyed?**

- In 1996, the US and other countries called for the final destruction of smallpox, but agreed to delay pending further science about new diagnostic tests and treatments for the disease. In 1998, with bioterrorism on my mind, I instituted an interagency process to review all of the issues to see if there was any reason to change our position. The next step is a Spring report from the Institute of Medicine at the National Academy of Sciences.

- We can never know whether destroying the two known stocks in Russia and the U.S. will eliminate the virus from the planet; there is a chance that some terrorist group or state may still hold clandestine smallpox virus and possibly even use it as a weapon in the future.

**Is the current U.S. stockpile of smallpox vaccine adequate? Should we be thinking about routine vaccination of the American people against such threats as anthrax and smallpox?**

- The US has enough good vaccine to protect millions of people, should we have to immunize persons exposed to smallpox from whatever source. Because that vaccine is old and slowly degrading, however, I have made the development and production adequate amounts of a newer vaccine a high priority.
- Mass civilian vaccination must involve a careful consideration of the risks and benefits. Bioterrorism is still low-probability. Also raises questions about some people who react adversely to such vaccines; the limited availability of the vaccines, and the high costs.

**Isn't public health a local problem? What is the appropriate federal role?**

- Public health is most often the responsibility of states and locals. But bioterrorism is a national security issue. The existing state and local structures will be used, but they will be helped by federal government expertise and funding.
- We will use local capacities to respond to a terrorist act, the Metropolitan Medical Response Systems. For chemical attacks, we need to provide immediate care at the scene. For biological attack, we need the local ability to detect a release, the ability to use our stockpiles, and the ability to treat those who become ill.
- Through the CDC in Atlanta, we will intensify our efforts to upgrade national public health capability to counter bioterrorism.

**What role does biomedical research have to play in countering bioterrorism? What are some longer-term R&D needs?**

- Near term needs are techniques for detection of organisms used in a bioterrorist attack, new and improved vaccines, and new and improved drugs to treat anthrax, plague, tularemia, and smallpox. Long term: generation of genetic information on potential bioterrorism agents.

**The military is already heavily involved in BW research and response. How does its activities differ from those you are doing in the civilian sector?**

- Civilian population is significantly more diverse in terms of age and health. List of agents that might be used in the civilian population is larger than that of military biologic weapons. Excellent collaboration between the military and civilian sectors on this problem.

## **GENERAL TERRORISM Q&A**

**In retrospect, wasn't it a mistake to blow up that pharmaceutical plant in Sudan?**

- What should any President do when he learns: a terrorist group has killed Americans. It announces it will kill more Americans. It announces an interest in chemical weapons. You know Iraqi Army chemical specialists are in Sudan. You know a plant capable of making CW in Sudan has a past history of association with the terrorist group. You know that the government of Sudan has a past history of association with the terrorist group. You then learn that a good scientific test has indicated the presence of a chemical compound only found in Iraqi nerve gas. Those were the facts.

**Why can't you get this one man, bin Ladin, before he kills more Americans?**

- We have a pretty good record of getting indicted terrorists. In jail now are the people who attacked the World Trade Center, those who tried to attack the Holland tunnel, the man who killed people at the CIA Gatehouse, those who plotted to blow up an aircraft in the Philippines. Last year we arrested a terrorist overseas who attacked us seven years ago.
- I can't tell you everything we are doing to deal with the threat from the bin Ladin network, but it is a very major effort.

**Can you ever win the war against terrorists? Won't they always be there?**

- Historically, there have always been such groups. At the beginning of this century there were Anarchists. There may be some correlation between levels of activity by such groups and periods of social, cultural, or technological change. The Post Cold War period, the opening of the Information Age, may be one such period in some countries.
- I do not agree, however, that we have to accept some level of terrorism. As new terrorist groups or new methods of attack emerge, we need to adjust to suppress the violence and increase safety. We did this, for example, with airplane hijackings. We are trying now to be ahead of the threat in chem-bio and cyber attack.

**Even your supposed allies do not support you when there is a terrorist attack, like the Saudis who have not cooperated in the investigation of the Khobar Towers bombing. Is that case ever going to be solved?**

- The Saudis have cooperated well on the Khobar case. Admittedly, there were some initial problems between two very different criminal investigative systems, but we worked that out. It is an active investigation, an open case with high priority. I can't say more than that.

**After ten years, aren't you now giving in to Libya on Pan Am 103?**

- No. We have always sought a real trial under American or Scottish law. If it makes Libya feel better to have it in the Hague, fine. But it must be a real trial, under Scottish law.

### **Isn't terrorism just the symptom of the cultural war between us and Islam?**

- No. We do not have a culture war between America and Islam. But let us be clear: there are those who attempt to steal religions, distort and wrap themselves in religion, and portray their enemies as enemies of their religion. Such men are frauds and blasphemers.

### **Why not change the executive order and allow assassination?**

- We do not want to encourage assassinations. We have all the authorities we need to take appropriate action against threats.

## **CBW PROLIFERATION Q&A**

### **What is the U.S. doing to help prevent former Soviet BW scientists from assisting the Iranian BW program?**

- US government has provided some \$30 million over the last five years to prevent proliferation of technology and expertise from former Soviet BW program.
- Seeking more than \$150 million in additional funds over next five years to continue and expand these efforts as part of the enhanced threat reduction program announced in State of the Union.
- U.S. programs creating greater openness at former Soviet BW facilities.
- For example, we're engaging former BW scientists at more than dozen Russian institutes in cooperative research in areas such as public health and vaccine development.
- Assisting Russian institutes explore commercialization opportunities with U.S. companies.
- Also helping to upgrade physical security at Russian biological institutes and eliminate BW infrastructure in Kazakhstan.
- US programs involve range of agencies: State, DOD, DOE, HHS and even Dept Agriculture. All activities designed to reduce risk that former Soviet BW facilities contribute directly or indirectly to BW program of Iran or other countries of proliferation concern.

### **Has the CBW threat grown?**

- With breakup of Soviet Union, threat of deliberate CBW attack from Moscow has all but been eliminated. Number of others outside Europe, such as Iran, Iraq, Libya and Syria, continue to threaten U.S. interests with their CBW programs.
- Most of these programs emerged during Cold War, but received little attention because of more direct Soviet CBW threat.

**Is it really possible to prevent countries from acquiring CBW?**

- U.S. export control and interdiction efforts making it much more difficult for proliferators to acquire CBW-related materials. For example, the Intelligence Community has publicly acknowledged that these efforts have set back the Libyan CW program by some 10 years.

**Aren't arms control treaties incapable of stopping proliferation programs?**

- No. Arms control can help cap and roll back proliferation programs. That's why pressing to complete substantive work this year on compliance protocol to strengthen 1972 Biological Weapons Convention. Want to put in place effective system of declarations and on-site activities to help deter countries from developing/producing BW.
- Chemical Weapons Convention in force less than 2 years, but 121 countries already renounced CW and at least 2 (South Korea and India) declared previously secret programs. Need to ensure CWC's implemented effectively.

**CYBER TERRORISM Q&A**

**Where is the threat? Are countries like Iraq and terrorist organizations preparing to use information warfare against the United States?**

- I won't go into any specific details on countries, organizations or their capabilities. Let me just say that we have intelligence that makes us think that it is essential that we start defending our critical computer systems.

**Where is our offensive capability in this?**

- I won't comment on any of intelligence capabilities.

**Russia has called for an agreement to ban information warfare. Why is the U.S. objecting?**

- We are working with Russia and the G-8 on cooperative arrangements to thwart terrorism and international crime., including computer crime.

**As I understand you, Americans will be vulnerable for at least five years. How is that OK?**

- We are much better off today than we were just last February when the so-called Solar Sunrise attack occurred on Pentagon systems. We are ramping up our efforts to thwart the threat that may develop over the next five years.

**If you do this right, won't you have to intrude on civil liberties?**

- No. My instructions are clear: defend America's cyber-space without diminishing our privacy rights, civil liberties, or proprietary rights. I am confident we can do that.

**If the private sector gives the federal government info, won't they open themselves up to leaks about their business operations?**

- We recognize that some companies may not want proprietary information given to the government. That is why we proposed a "cut out" that would strip out the names of companies and such information and share with the government experts just the nature of the cyber problems, so that we can help with the any special knowledge we may have.

**But you're asking private businesses to work with the FBI, perhaps the last place they want to go. Isn't the National Infrastructure Protection Center just the FBI in sheep's clothing?**

- The National Infrastructure Protection Center is an inter-agency organization housed at the FBI. It is represented by government employees reflecting numerous agencies throughout the federal government. It is one part of part of our effort. The National Plan to defend cyber space is being prepared by an interagency team housed in Commerce. This is not just a law enforcement issue. It is about insuring that our economy can continue to work.

**So much of the critical infrastructure is privately owned. Won't excessive government regulation to impose security standards on the private sector hinder economic growth and innovation?**

- We have no plans for imposing security standards on the private sector. The innovation is really in the public-private partnership envisaged in the PDD whereby a cooperative effort on the part of industry and the federal government would ensure the security of our critical infrastructure systems.

**Big companies like Microsoft are having real problems recruiting enough people with computer skills. How can the federal government compete?**

- This is a real problem. Also problem that our colleges aren't producing enough computer experts. To help solve both problems I am creating Cyber Corps, a ROTC-like program to exchange college scholarships for commitments to government service. The Cyber Corps administration will start in FY00, the first scholarships will be given out in FY01.

**Isn't your encryption policy related to our national defense against cyber terrorism?**

- We need to solve the encryption issue in a way that addresses both the law enforcement and the commercial requirements. I think we can. But, threats to information systems exist outside of the encryption debate. The vulnerabilities to disruption of critical services, corruption of data and the degrading of defense systems go beyond encryption technology.

**How does all this relate to Y2K? Do you expect a disaster?**

- Y2K has taught us all the extent to which we are now dependent upon computers to make virtually everything work. Just as Y2K, left unaddressed, could have brought things to a halt so too perhaps could a cyber attack someday unless we address that threat.

- I am confident there will not be a disaster in the US. There may be unanticipated problems, but we will be ready to deal with them. My concern is that some other countries are realizing too late that this is no joke.

**Your own Marsh commission called for increased R&D but there has been little support for increased funding. Your PDD called for the government to be a model for the private sector and yet early last year the Department of Defense was caught completely off guard against an information system attack. Why is the federal government so behind the curve?**

- In fact we have increased federal funding for research and development totaling \$500 million for FY00. We are at the beginning of a concerted effort to bring the federal government up to the technological edge of information security and are proactively addressing an emerging threat before it has arrived. The DoD experience taught us valuable lessons about the need for better defenses and is the principle reason we are funding these efforts.

C

# Germ Weapons: In Soviet Past Or in the New Russia's Future?

## Recent Findings About Old Programs Spur Doubts in the U.S.

By JUDITH MILLER  
and WILLIAM J. BROAD

Just as the Soviet Union was ending its confrontation with the West in the late 1980's, the military officers who ran Moscow's secretive germ warfare program ordered up new, much deadlier arms.

At a remote laboratory complex in Kazakhstan, Russian scientists began animal testing of the Marburg virus, a highly contagious germ that kills by attacking every organ and tissue in the body.

This secret testing, described recently by several veterans of the Soviet program, went undetected at the time by Western intelligence agencies, which knew few specifics about the plant's operations.

Kazakhstan gave up nuclear, biological and chemical weapons soon after it became independent, and permitted American experts and a handful of reporters to visit the plant. From their observations, and from Soviet defectors, the West has finally learned what was unfolding there in the final years of the cold war.

The belated discovery of this exotic arms research is one of the elements of a fierce dispute in Washington over whether the Russian military is heeding President Boris N. Yeltsin's 1992 order to abandon germ warfare.

Similar uncertainties loom about Iraq. With the apparent end of United Nations inspections, the West is now trying to track Baghdad's germ work with satellites and, perhaps, spies — the same methods that failed to unmask the Soviet program.

Clinton Administration officials contend that Russia no longer poses a major threat. Western experts have visited most of its key civilian laboratories, and officials disclosed that Russia had recently moved closer to allowing Western experts to visit its closed military installations, a crucial step that could dispel many of the lingering doubts about Moscow's activities.

Administration officials assert that much of what they now understand about the Soviet Union's germ weapons has been gleaned through Western aid programs intended to foster peaceful research projects. Those projects also pay salaries to former germ scientists, fending off

what officials say is the gravest danger from the Soviet program — recruitment of scientists by rogue states or terrorists.

But some Administration officials and Republicans in Congress assert that Russia is still secretly researching germ weapons, just as it did in the cold war.

Congress recently cut spending on the cooperative exchanges with Russian germ scientists from \$14 million to \$7 million, both because of persistent doubts about Russian intentions and to punish Moscow for selling nuclear and missile technology to Iran.

The debate turns partly on history. After developing germ weapons for several decades, the United States and Russia signed an international treaty in 1972 banning such arms. Almost immediately, Soviet defectors say, Moscow secretly redoubled its germ research and production.

Officials and lawmakers acknowledge that there is scant hard evidence to support their suspicions that Russia is cheating again, but point to Moscow's reluctance to open up its military bases as an ominous sign.

That may be changing. Two weeks ago, the officials said, a small group of Pentagon experts and senior defense scientists met their Russian counterparts for the first time at the Military Academy of Radiological, Chemical and Biological Defense, a once-closed military training institute in Tambov, some 300 miles southeast of Moscow.

High on the agenda were possible scientific exchanges that may provide direct Western access to Russia's biological "holy of holies," as one official put it, four military installations at the heart of the Russian germ empire — Sergiyev Posad, Kirov, Yekaterinburg (Sverdlovsk), and Strizhi, none of which has been visited by the West.

Officials said the military teams had agreed in principle to a series of military exchanges, starting in the United States sometime next year.

"This is the beginning of a long process," said an official who spoke on condition of anonymity. "But the ice has finally been broken, and it's now clear that both of us want to do business."

The breakthrough is potentially significant. Iraq's entire germ arsenal contained enough deadly poison at its peak to kill all the people on earth many times over, according to United Nations weapons inspectors. Yet, the Iraqi program was dwarfed by the amount and variety of weapons the Soviet Union had secretly amassed.

The Soviets, as suggested by their research on the lethality of the Marburg virus, were racing ahead in their final days to develop entirely new classes of weapons.

With more than 60,000 scientists and experts at work, they were also developing compounds that could control human moods, heart rhythms and sleep patterns and that could be used to destroy an enemy

army. Among the many unanswered questions, American officials say, is where such work stands today.

## Kazakhstan's Past

### City of Death Tries to Stay Alive

Stepnogorsk, in Kazakhstan, was the only major Soviet germ installation outside the Russian heartland. Called the Scientific Experimental and Production Base, it was known only by its post office box, No. 2076.

While Western intelligence analysts had deduced from the configuration of the buildings that it was designed to produce anthrax or other bacteriological agents, they never figured out precisely what the kind of research was being done, what weapons the factory was making or what threat it posed.

Built on a huge scale on a desolate, wind-blown steppe of Central Asia, it is an eerie place to visit. The security fences are no longer electrified. Air locks hang open. Plastic floor covers installed to ease decontamination are torn and buckling from neglect and the cold.

Six stories high and two football fields long, the central factory there is filled with 10 giant fermentation vats, each meant to brew 5,000 gallons of anthrax microbes — enough to kill every man, woman and child in America many times over. Iraq's entire germ production could have just about fit into one of those vats. And Stepnogorsk was only one of six such Soviet plants.

"As you can see, we haven't made that in some time," Gennadi L. Le-

pyoshkin, the base's director, told Pentagon experts and a reporter who recently walked through the anthrax plant, which is being dismantled with Pentagon aid. "And we will never do it again."

Russian workers began building the complex in 1982. Former Soviet officials say it was a replacement for Sverdlosk (now Yekaterinburg), the Russian military installation where, in 1979, an accidental release of anthrax microbes killed about 70 people as well as livestock up to 30 miles away.

Its role in the confrontation between the superpowers remains unclear. Kanatjan Alibekov, or Ken Alibek, as he is now known, Stepnogorsk's former director who defected to the United States in 1992, says the plant was to produce up to 330 tons of final "product" in a 200-day period if the order came to mobilize for war.

To this day, however, Moscow says Stepnogorsk made only vaccines and other defensive germ products. But Russian scientists who worked there in Soviet days and now run the place say otherwise. "This plant was an integral part of the Soviet germ weapons program," said Dr. Le-pyoshkin, the former Soviet colonel who now heads the National Center on Biotechnology in Kazakhstan.

Moreover, the remaining physical evidence of its real purpose is impossible to hide. Next to a concrete bunker is a machine that Dr. Alibek said was for filling and sealing bomblets. Such equipment — what a Pentagon official called "a smoking gun" in that it proves the factory produced weapons, not vaccines — had never previously been discovered at a Russian germ installation.

Since 1996, Washington has been trying to help Kazakhstan convert the installation to peaceful work through a low-key, \$5 million program. But the effort has moved slowly. Financial aid was tied up until last spring when Kazakh officials finally stopped demanding that Washington fork up \$12 million for unpaid utility bills and pay taxes on its assistance.

Commercial success will not be easy, experts say. Stepnogorsk is extremely isolated and, as of last month, had food shortages and little or no heat. The city's airport is moth-balled, as are the only hotel and movie theater.

Last March, a well-equipped toxicology lab there opened after an infusion of more than \$750,000 in American aid. The lab employs about 60 former germ scientists who have begun producing, among other things, vials of burn ointment.

Other former employees are struggling to make a living in the impoverished town of 70,000. "Hope dies last," said Sergei Antonovitch, a former germ plant scientist who now owns a poorly stocked pharmacy in town.

## Russia's Future

# U.S. Tries to Plumb Moscow's Intentions

While Kazakhstan has dismantled its germ program, doubts persist about Russia.

Moscow's lies about the issue during the cold war, skeptics in Washington argue, make trust and cooperation impossible. Supporters of the Western programs say they do not blindly trust Russia, but feel that partnership is the best chance for

verifying Moscow's claim to have renounced germ weapons.

Skeptics note that Mr. Yeltsin has banned Russian experts from discussing any aspect of their country's germ history and has retained several generals instrumental in the Soviet program.

They worry, particularly, that research may be quietly proceeding on some of the least known of the Soviet advances: "bio-regulators." This work was aimed at creating germ agents that could take control of human functions like moods, heart rhythms and sleep patterns.

Dr. Igor V. Domaradskizh, a pioneer of the Soviet program, said in a recent interview that his scientists were searching for compounds that could "sharply change a person's behavior or emotions, such as causing fear or an ultra-rapid heartbeat."

As far as is known, they did not succeed. But Dr. Domaradskizh said biological science had now progressed to the point where "it can be done."

Dr. Alibek, the former germ scientist who once ran the plant in Kazakhstan, is critical of part of the West's approach. The Soviet germ program was hidden in a myriad of civilian and military institutes. Even Soviet intelligence, the K.G.B., he disclosed, had its own germ centers, which developed agents for assassination under the code name Flayta, or Flute.

Some of Moscow's former germ scientists, he said, have recently published papers that could conceivably aid weapons research, including several about cultivating the deadly Marburg virus.

Russia, Dr. Alibek insisted, will never entirely abandon a program in which it had military superiority, no matter how many treaties it signs or cooperative programs it joins. "I say, 'Guys, don't be so gullible. They're lying to you,'" he said.

Representative Floyd D. Spence, the South Carolina Republican who heads the House Committee on National Security, contended that even civilian biology partnerships might be dangerous if they helped sustain Russia's germ establishment.

Administration officials say those exchange programs are already showing beneficial results. Those

who follow the program most closely say that there is no evidence of large-scale activity even at the military institutes. And one American expert, who spoke on the condition of anonymity, said Russia's economic turmoil made large-scale germ work unlikely.

"Maybe there is a well-lit, well-heated, well-funded military lab out there that is just humming along, totally insulated from the cutbacks that have slashed funding for military salaries and other critical Russian defense needs," he said. "But I don't believe it."

Top Russian scientists deny that Russia still has a germ weapons program. "Everything has been destroyed, on our side and yours," said Nikolai N. Urakov, a former Soviet general who heads a converted germ center at Obolensk that now does research for peaceful purposes.

Former Senator Sam Nunn, the Georgia Democrat who helped sponsor legislation authorizing the scientific exchanges and recently toured Obolensk, said the ambiguity about Russia's germ program would persist because much basic biological research has both civilian and military applications.

"This is not something you see with a satellite," he said. "It all turns on intent. That's why this is such a hard intelligence problem."

But the gamble, he said, is worth the risk.

"We still don't know, and won't know for many years to come, whether or not we succeeded," Mr. Nunn said recently in Moscow. "But we do know that while we can argue about whether the glass is half full or half empty, we know that the trend is right. A decade ago, the glass was all empty."

# The Threat of Germ Weapons Is Rising. Fear, Too.

Sunday, December 27, 1998

By WILLIAM J. BROAD  
and JUDITH MILLER

**A**MERICAN troops in the Persian Gulf are vaccinated against deadly germs. So are Federal Bureau of Investigation agents who are probing a growing number of biological incidents. So are some White House officials.

Protections against living weapons are new to the military and security of the United States, and they raise troubling questions.

Is this prudence or paranoia? Should everyone be vaccinated? How real is the threat? Aren't deadly germs nearly impossible for attackers to use without hurting themselves? Isn't this threat just another bogeyman, like so many before?

Germ weapons, though around for centuries, have played no significant role in modern warfare and terrorism. Skeptics point to this history and say that biological strikes of any consequence are unlikely.

But officials in Washington from President Clinton on down are taking the issue very seriously, with thousands of people and billions of dollars in motion to address the germ threat.

"Eventually, this is going to hurt us," said Robert M. Blitzer, who recently left the Federal Bureau of Investigation after directing its section on domestic terrorism. "There's no question in my mind."

Moreover, a yearlong inquiry by The New York Times revealed trends that suggest the era of germ tranquility may indeed be ending:

- Uprooted weapon scientists from Iraq, Russia and South Africa are hunting for new jobs and spreading germ secrets.

- Radical states with reputations for supporting terror, such as Iran and Libya, are seeking germ weapons.

- Terrorists, including Osama bin Laden, are increasingly interested in pestilential germs. Some boast openly of being able to kill foes with deadly plagues.

Today, officials in Washington stress that they know of no imminent danger, even while acknowledging the limitations of intelligence. Most agree that the threat, while low, is growing.

The defenses that Washington is quietly erecting, officials say, are akin to the insurance that homeowners take out against floods and earthquakes. The odds may be small, this argument goes, but precautions are warranted since conditions are changing and damage could be great.

R. James Woolsey, Director of Central Intelligence from 1993 to 1995, is among the former officials who are worried. Germ terrorism, he said in an interview, is "the single most dangerous threat to our national security in the foreseeable future."

## The Munitions

Germ weapons can be hard to make and use, contrary to myth and claim. It took the United States decades to master the art before renouncing such arms in 1969. In the early 1990's, Aum Shinrikyo, a Japanese cult, launched at least nine germ attacks in Tokyo that were meant to kill millions. But the strikes produced no known injuries or deaths.

Dangerous to the attacker as well as the attacked if successful, germ weapons are considered most practical when used far from the aggressor's homeland; intervening land and air can abolish what amounts to a

quarantine.

The main appeal of such weapons is that they are incredibly cheap compared to chemical and atomic arms. Yet pound for pound, germ weapons rival nuclear ones for maiming and killing, and some biological agents are considered superior in that regard; in theory they can annihilate many millions of people.

Clearly, they surpass their nuclear kin as an instrument of fright and disruption: Once sown, infections can spread unpredictably, since they are alive. Experts especially worry about smallpox, which is highly contagious and seen as particularly dangerous since few people are now immunized against its ravages.

"To say the threat is low is not to minimize its potential," said Neil J. Gallagher, assistant director for national security at the Federal Bureau of Investigation.

## The Supply

Today, the secrets of germ warfare are increasingly up for grabs as weapon scientists from countries that made biological arsenals hunt for new jobs. The nomads are from Iraq (starting in 1991 after Persian Gulf war), Russia (starting in 1992 after the Soviet collapse) and South Africa (starting in 1994 as apartheid fell apart). Russia alone has many thousands of former germ warriors increasingly cold, poor and hungry.

Legitimate science also heightens the risk. The global war against infectious disease has produced more than 1,500 germ banks that tend to trade freely in deadly microbes.

Future strides could make matters even worse. Experts agree that research into the genetic foundations of life, an approach that promises to cure many diseases, might, in evil hands, one day produce weapons that work against only certain races or ethnic groups.

"It's difficult but not impossible," said Dr. Joshua Lederberg, a Nobel laureate in biology who advises Washington on germ warfare. More unsettling, he added, is that traditional killers seem to be a growing danger right now; he called them "a monster in the back yard."

## The Demand

Today, at least 17 nations are suspected of having or trying to acquire germ weapons. Perhaps they want to deter foes. The wild card is that some (Cuba, Iran, Iraq, Libya, North Korea, Syria) are also considered architects of terrorism.

Libya worked hard to join the germ club. In 1994, it sought to hire scientists fleeing South Africa's crumbling program, including its head, Dr. Wouter Basson. That move, officials say, was foiled by diplomatic pressure from Washington and London.

However, Libya may have succeeded in hiring (or perhaps hiding and employing for Baghdad) Dr. Amir Medidi, a top scientist of Iraq's germ effort, United Nations inspectors revealed.

Terrorists themselves seem increasingly drawn to germ weapons.

Osama bin Laden, the renegade Saudi millionaire known for his bitter hatred of America, is investigating them, American officials say. Whether his work has resulted in secret laboratories or usable arms, no one in Washington seems to know or is willing to say.

Nasser Asad Al-Tamimi, an Islamic radical, has

*Continued From Page 1*

been vocal. Early this year Al-Balad, a Jordanian newspaper, quoted him as saying that "jihad" had at last discovered how to win the holy war — lethal germs.

Disturbingly, growing interest abroad is shared by domestic radicals and militia groups at home. Catalogues catering to them carry ads for such books as "Guide to Germ Warfare."

Larry Wayne Harris, an Ohioan with a history of hate-group affiliations, was arrested in 1995 for having bought plague bacteria from a germ bank under false pretenses. A registered microbiologist, he now says the microbes were strictly for defensive purposes.

"There are groups all over the world after this kind of stuff," Mr. Harris said, his blue eyes icy. "You're not going to stop germ warfare. The only thing to do is defend yourself."

## The Assessment

Intelligence experts say knowing the truth is hard. Spies and satellites are only marginally helpful for ferreting out biological gear as small as kitchen cookware that is easy to hide and whose purpose can be peaceful (unlike the nuclear arms, bombers, ships, missiles and factories that dominated the cold war). Even hundreds of arms inspectors in Iraq, who probed that nation for seven years, ended up with as many questions as answers.

Moreover, the attention focused on germ warfare has already helped give rise to germ hoaxes, and experts worry that serious concern might give way to complacency. This year, the Federal Bureau of Investigation is fighting a wave of false anthrax threats in letters mailed to abortion clinics.

Federal officials note that Ramzi Ahmed Yousef, mastermind of the 1993

World Trade Center blast, which killed six people and injured more than 1,000, claimed that his goal was to have one tower fall into the other and kill a quarter million people — more than died in the atomic bombing of Hiroshima.

A top former official disclosed that Mr. Yousef, when arrested in 1995, was found to have been studying not only chemical but biological weapons.

John C. Gannon, chairman of the National Intelligence Council of the Central Intelligence Agency, last month told a Stanford University meeting that the danger of germ and chemical devastation is rising.

He warned that terrorists and foes with such weapons are growing in number and that the increasingly lethal agents they are developing "have the potential to cause massive casualties."

## The Response

Federal officials are struggling to tighten commerce in germs both at home and abroad. President Clinton himself recently raised the issue at Camp David with Fernando Henrique Cardoso, the President of Brazil, who has begun a program to restrict germ sales.

In Russia, Washington is expanding cooperative programs meant to keep former germ warriors in place doing peaceful research.

In NATO, Washington is arguing that the Atlantic alliance should take the lead in a global fight to stop terrorists from getting or using germ weaponry.

Meanwhile, the American military is vaccinating all troops against anthrax, which causes high fevers and death, and has begun a \$322 million program to build stockpiles of 18 other vaccines, including one against smallpox. Recently, Congress approved \$51 million to start building domestic stockpiles of medicines and antibiotics, especially for police, fire and health workers.

Physical security at key Federal buildings is being enhanced to foil terrorists who might try to spread deadly germs and chemicals through the air. The steps include ventilation improvements so a gentle breeze blows outward whenever a door or window is opened. In theory, this so-called positive pressure will automatically sweep away dangerous agents.

Across the country, Federal officials are holding seminars in the nation's top 120 cities to train emergency personnel.

More broadly, intelligence agencies are struggling to monitor terrorists more closely. The Federal Bureau of Investigation's nightmare is talented loners, who are difficult to track.

The Pentagon is weighing whether to ask the President to authorize appointment of a military commander who could plan and direct operations to defend the continental United States in the event of germ chaos, a step beyond the civil defenses of the early cold war. No such commander's post now exists.

"Within minutes of an event, people

are going to turn to us," John J. Hamre, the deputy Secretary of Defense, told a meeting of military officials in explaining the need for homeland defense. "It could get crazy very fast."

To date, there has been little public debate over the risks and benefits of such actions, partly because the many responses to the germ threat have been both quiet, to avoid frightening Americans, and piecemeal.

But that may change as echoes of bomb shelters start to reverberate and as Washington scans the horizon to better judge the danger in the years and decades ahead.

Tension is sure to rise between the need for protection and "rights to privacy, something that we hold very dear," Defense Secretary William S. Cohen recently told the Council on Foreign Relations. That kind of friction, he added, will force "unpleasant choices" in the near future. "We haven't really faced up to it yet."

# Germes, Atoms and Poison Gas: The Iraqi Shell Game

By WILLIAM J. BROAD and JUDITH MILLER

**S**OMETIMES past is prologue. As Iraqi officials in 1995 led United Nations arms inspectors to a large cache of documents hidden on a chicken farm near Baghdad, a red photograph album stood out. At first glance, the album, like the half million pages of other papers in the shed, seemed to cast light on Iraq's secret drive to obtain germ, chemical and nuclear arms and missiles.

But closer scrutiny revealed huge gaps. The album's dozens of pages, for instance, offered some insights into Iraq's germ efforts. Photo after captioned photo showed not only flasks of deadly agents like anthrax but animal test subjects small and large, including sheep.

Yet the inspectors found that the album covered germ work only through 1989 — before Baghdad embarked on a crash program to turn experimentation into weapons for the 1991 Gulf war, in which it deployed germ bombs and warheads at four sites, but did not use them.

Moreover, something else was missing. The numbered pages were interrupted where photos had been removed from the three-ring binder.

"We don't know what was taken," one inspector said. "My guess? Pictures showing people" central to

building the arsenal.

Today, seven years after President Saddam Hussein promised to come clean about his weapons of mass destruction, the book on Iraqi arms is still full of holes.

Military experts in Washington and at the United Nations say the unanswered questions are serious and legion. Still unaccounted for are hundreds of chemical arms, tons of nerve gas, more than 100 germ weapons and parts for up to four nuclear warheads, which are said to lack only the uranium to fuel them.

"There are vast areas of activity that are still unknown to us," said Gary Milhollin, director of the Wisconsin Project on Nuclear Arms Control in Washington and an expert on Iraq's arsenal. "The uncertainties are so great that, as far as we know, Saddam Hussein today could have both chemical and germ warfare agents in warheads, ready to go."

Mr. Milhollin and his staff have prepared a list of some of the main riddles about Iraq's unconventional weapons. Their chart, below, is lengthy. Yet Mr. Milhollin and United Nations experts note that no such list can be exhaustive. Given Iraq's evasiveness and defiance, its stonewalling and lies, such listings can only suggest the depth of the remaining questions.

"This is not definitive," one inspector said of the chart, adding that the goal was out of reach even of the

United Nations and Federal intelligence agencies.

Prospects for greater illumination are bleak, analysts say, because of both the unknown consequences of the bombing that began Wednesday and Baghdad's obstinacy. What evidence might have been destroyed in the bombing was unknowable, but the inspection process, most analysts agree, had all but collapsed.

**R**ICHARD BUTLER, chairman of the United Nations Special Commission in charge of arms inspectors in Iraq, is more diplomatic. "It must regrettably be recorded again," he told the Security Council on Tuesday, "that the commission is not able to conduct the substantive disarmament work mandated to it."

The stakes are potentially huge. Iraq has already confessed to having made enough deadly microbes to kill all the people on Earth several times over. And Saddam Hussein has used weapons of mass destruction before.

After losing the 1991 Gulf war, Mr. Hussein, as a condition of surrender, agreed to declare within 15 days all his nuclear, chemical and biological arms and the missiles for delivering them, and then to destroy them.

The United Nations set up a group to insure that he kept his word. Until it verified destruction of the weap-

ons, Iraq was barred from selling oil. Later, the United Nations relented a bit and allowed some oil exports to pay for food, medicine and war reparations.

To date, those sanctions have cost Iraq more than \$120 billion. Eager to escape them, Baghdad over the years has offered at least five different "full, final and complete" disclosures, but the United Nations officials have dismissed these as woefully incomplete.

An example of Iraq's pale cooperation is demonstrated in the 1995 chicken-farm haul, which was one of the special commission's greatest finds. While the documents were valuable, they had been carefully culled and included nothing from the headquarters of the Military Industrialization Corporation or the relevant archives of the Ministry of Defense.

Among the ugliest outstanding questions is whether Iraq tested its germ weapons on people. Rumors and even some suggestive photographs have come to light. But so far, there is neither proof nor admissions.

Recently, the battle for truth about Iraq's armaments has been crippled by diminishing returns.

The latest round of inspections aimed at testing Iraq's compliance with United Nations resolutions was an abject failure. In interviews, inspectors told of astonishing Iraqi feints and what one non-American inspector called a saga of "lies and deception."

"All the News  
That's Fit to Print"

# The New York

VOL. CXLVIII . . . No. 51,365

Copyright © 1998 The New York Times

TUESDAY, DECEMBER 8, 1998

## Bio-Weapons in Mind, Iranians Lure Needy Ex-Soviet Scientists

By JUDITH MILLER  
with WILLIAM J. BROAD

MOSCOW — Iran is scouring the former Soviet Union to hire scientists who once worked in laboratories tied to Moscow's vast germ warfare program and has succeeded in recruiting some of them to take jobs in Teheran, according to Russian scientists and American officials.

Iranian officials who report to their leadership have approached dozens of scientists who once made germ weapons, offering as much as \$5,000 a month to people who make far less than that a year in the increasingly chaotic Russian economy.

Russian scientists say most of these entreaties have been rebuffed. But they acknowledge that at least five of their colleagues have gone to work in Iran in recent years. Others have accepted contracts that allow them to continue living in Russia while conducting research for Teheran, the scientists said.

In interviews in Russia and neighboring Kazakhstan, more than a dozen Russian former germ scientists reported contacts with Iran, and two said they had been asked specifically to help Teheran make biological weapons. American officials say many more Russian scientists have disclosed such contacts and believe that Iran is developing a germ arsenal.

Iran has powerful reasons to want such weapons and even ex-

### THE GERM WARRIORS

*A special report.*

pressed interest in acquiring them a decade ago. Most Iranians believe that Iraq used biological as well as chemical weapons in the Iran-Iraq war in the 1980's, and many countries in the region, including Israel, Syria and Iraq, are suspected of having germ arsenals.

Gholamhossein Dehghani, counselor to Iran's mission to the United Nations, said many foreign scientists worked in his country, but were doing only peaceful research. He also stressed that Iran had ratified a 1972 international treaty banning germ warfare. He said he "categorically rejected" the claim that Iran is hiring Russian biologists to work on germ warfare. "We do not believe that having such weapons increases our security," he added.

Other Iranian officials have also said Iran's research is not offensive. But veterans of the Soviet and American germ programs dismiss such claims.

"It's often hard to distinguish between a drug and a weapon, or between offensive or defensive research," said Lev S. Sandakchiev, director of Vector laboratory, which made deadly viruses for weapons in Soviet times. "What counts is intent. And that compli-

cates trust."

American officials say Teheran's successes are troubling because they suggest that knowledgeable scientists — the key to Russia's once-secret germ arsenal, which at its height employed some 70,000 scientists and technicians — could be recruited by anyone with enough influence or cash, including rogue states and even terrorists.

An important figure in Iran's buyer network, Russian scientists and Western officials say, is Mehdi Rezayat, an English-speaking pharmacologist in Teheran whose business card, provided by a Russian scientist, says he works for President Mohammad Khatami as a "scientific adviser."

Russians approached by Dr. Rezayat and other Iranians say their recruitment style alone raises suspicions. Visiting delegations, they said, are sometimes led by Iranian clerics, who wield ultimate power in Iran's theocracy, and other nonscientists who are studiously ambiguous about precisely what they want the Russians scientists to do.

Moreover, the Iranians on other occasions have shown particular interest in learning about microbes that can be used in war to destroy or protect crops, as well as genetic engineering techniques key to both legitimate research and the making of deadly germs for which there may be no antidotes.

American officials assert that Teheran's biowarfare program may already have turned some germs and toxins into weapons, but they have scant information on Iran's progress. There is direct evidence, the officials said, that Russia has significantly improved Iran's missile and nuclear capacities, but the value of Russian biological aid is less clear.

"Outside assistance is both important and difficult to prevent, given the dual-use nature of the materials and equipment being sought," the Central Intelligence Agency said recently in a report on Iran and its effort to make germ weapons.

To counter Iranian and other recruiting, the United States has quietly begun an effort to become the largest and best-funded competitor for the allegiance of Russia's former germ scientists. Washington is sponsoring search projects, and programs to convert to civilian use laboratories and institutes once associated with the Soviet germ program.

From a base of less than \$10 million, it expects to spend at least double that sum next year, trying to keep Russian scientists gainfully and peaceably employed at home, and to stymie efforts not only of Iran, but also of North Korea, Syria and China, to lure biological talent and technology.

"This is a high-stakes game to win the hearts and minds of Russia's best scientists, who are dangerous simply because of what they know," said Senator Richard G. Lugar, Republican of Indiana, who recently visited former Russian weapons sites now engaged in peaceful research.

Continued on Page A12

The business card of a major Iranian recruiter of Russian scientists specifies his link to the office of the Iranian President.

### Tehran Medical Sciences University

M. Rezayat, Ph.D.

Director Of Pharmacology Department

Scientific Adviser

Office Of Scientific & Industrial Studies Of Presidency

23, West Arash Blvd.  
Oxford St.  
P.O. Box 14155-4871  
Tehran 19100

Tel: 98-21-8900015-8402569  
Fax: 98-21-8900016  
Tx: 210537 0815 IR

## The Buyers

# Iranians Shop Far and Wide

Russian scientists courted by Iran describe what amounts to a fairly predictable recruiting pattern. First, they say, there is a call, sometimes from a Russian colleague, or a faxed letter from an Iranian scientist proposing a visit. Then there are initial discussions of vague scientific cooperation and hints of large sums of money.

At later sessions or in follow-up calls, letters and faxes, invitations to visit Iran are issued, and the Iranians begin discussing their needs more bluntly. Often, they said, the weapons question is raised through hints and implication.

Shortly after the Persian Gulf war, Russian scientists said, Iran tried to recruit Russian biological talent from leading germ laboratories. The effort largely failed, the scientists said, and Dr. Rezayat and other Iranian agents turned their attention to smaller institutes.

In an interview, Gennadi N. Lepyoshkin, former director of what was a sprawling germ weapons plant in Stepnogorsk, Kazakhstan, said Iranian middlemen had approached him in 1991, presenting themselves as entrepreneurs interested in establishing commercial contacts. "But their proposals were such that we immediately declined and ceased contact with them," said Dr. Lepyoshkin, whose plant once specialized in developing and producing anthrax weapons.

Scientists say the Iranians' 1997 visit to the All-Russian Institute of Phytopathology in Golitsino, just west of Moscow, was typical of approaches to smaller groups involved in the Soviet germ program.

Under Communism, the institute made pathogens for killing crops to starve enemies. But since the Soviet collapse it has struggled to do purely peaceful research. In the last seven years, its staff has dropped to 276 from 1,200, and it pays employees intermittently.

Despite the hard times, the institute has become a leader in pesticides research and in transgenic plants, whose genes are manipulated to resist certain herbicides, insects and diseases.

About a year ago, one of its scientists bumped into an Iranian while visiting a Moscow-based laboratory. It was Dr. Rezayat, whose business card described him as director of Teheran Medical Sciences University's pharmacology department and also as an adviser to the "Office of Scientific and Industrial Studies of Presidency."

"Rezayat seemed to have visited most labs and institutes in the area," recalled the Russian scientist, who invited him to Golitsino to meet his colleagues. Eventually a five-man Iranian delegation made the trip and met, among others, Yuri Spiridonov, a crop expert who is now head of the herbicide department.

The Iranians expressed great interest in scientific exchanges, Dr. Spiridonov said.

He told the Iranians he had no objection in principle to such collaboration. But the delegation made him nervous, he said. For one thing, only half of the Iranians were scientists. "The others just sat their with their

In addition, he said, they asked "troubling" questions about substances related to biological warfare. Dr. Spiridonov declined to elaborate.

"These were not scientific questions," he recounted 18 months later in an interview in that same office, now cold and poorly heated against the bitter Russian winter.

Wary of his guests' intentions and fearful of endangering his growing ties to Western scientists and companies, Dr. Spiridonov said, he declined invitations to visit Teheran or to discuss his research in any detail. But three of the institute's other scientists did travel to Teheran, and invitations keep coming — including another last week.

[Dr. Rezayat was reached by phone in Moscow on Dec. 6 and asked about allegations that he was helping recruit Russian scientists for germ warfare. He said he could say nothing without Teheran's approval, but added that such claims were both common and false. He promised to seek permission to comment. A day later, his assistant said that Dr. Rezayat was no longer in Russia.]

Western officials identify Dr. Rezayat as a key official in the biology branch of an Iranian intelligence office that covertly shops for talent and technology involving nuclear, chemical and biological weapons. It also has responsibilities for public health.

That office, said Ahmad S. Hashim, a Middle East expert who consults for the American Government, is well known for its relentless pursuit of expertise and technology in deadly weaponry, and not just in Russia. An American official agreed, saying, "They are definitely hunters."

## The Experts

# Scientists Describe Recruiting Techniques

One of the scientists Dr. Rezayat courted last year was Valery M. Lipkin, a biochemist and deputy head of the Shemyakin and Ovchinnikov Institute.

This center, built with Soviet Ministry of Defense funds, used to do research on vaccines and biological toxins. Though struggling financially, it still has valuable assets, including a laboratory for conducting advanced vaccine and other nonmilitary tests on animals.

In the summer of 1997, in the institute's branch in Pushchino, about an hour outside Moscow, Dr. Lipkin met with a six-man Iranian delegation that included Dr. Rezayat.

The Iranians seemed to defer to a senior cleric in a black turban and flowing robe, the Russians said.

His name was Mahmoud Hosseini, and his business card identified him in Russian as general secretary of the "Iranian Society's Office of Scientific-Technical Cooperation with the Russian Federation," based in Teheran. The Iranian Embassy in Moscow said Mr. Hosseini was a diplomat who held the

title First Secretary for Economic Affairs.

The meeting went well, Dr. Lipkin said in an interview at his sprawling Moscow headquarters, though some gangs struck him as odd.

He said the cleric, though well educated, was not a scientist. And though the Iranians spoke of possible exchanges of students and technology and seemed willing to pay handsomely for them, the delegation was vague about what it wanted.

"One thing they repeatedly asked about," said Sergei Feofanov, Dr. Lipkin's deputy, "was human genetic engineering."

In germ weaponry, the possibility of attacking human genes is the most chilling of all, military experts agree. In theory genetic engineering could produce weapons that kill or cripple selectively by race and nationality. Such developments, if possible, are years away.

During the next 18 months, the Iranians made three visits to the Shemyakin institute, Dr. Lipkin said. But they never responded to his offer to train Iranian students in Russia. Instead they bombarded the institute with invitations to younger researchers, asking them to teach genetic engineering and other advanced techniques in Teheran for a year or longer.

There was also a personal invitation faxed to Dr. Lipkin from Abbas Keshavarz, deputy chief of a research organization in Iran's Agriculture Ministry. It invited him to visit Iran to discuss possible "future collaboration." A copy was sent to Dr. Rezayat's office.

"I didn't want to discuss weapons," Dr. Lipkin said. "So I kept pressing them, 'What will I do in Teheran? What is my program?' But they would not tell me. And that made me nervous. For while they were cautious here, had I gone there, I think they would have raised weapons and other inappropriate topics."

Dr. Lipkin said that before saying no, he had sought advice from a friend at the Russian Ministry of Science, who warned him that an Iranian visa in Dr. Lipkin's Russian passport would not enhance his prospects for cooperation with American scientists. Especially a trip sponsored by Dr. Rezayat, the friend warned.

Iran has succeeded in attracting several Russian biologists to Teheran, said colleagues who identified them in recent interviews. One is said to be Dr. Valery Bakayev,

a senior biologist at the Institute of Medical Biotechnology in Moscow who accepted a teaching post in Iran more than seven years ago, a colleague said. A spokeswoman for the Moscow institute, which was once part of the germ empire, said she had no idea where Dr. Bakayev had gone after leaving his post.

Another scientist said Dr. Vladimir Rishinski, an expert at the Institute of Molecular Biology, recently took a leave of absence to go to Iran for two months of teaching, his second leave for that purpose. According to his institute, which Ken Alibek, a former senior Soviet official, said researched agents for germ weapons, he is "on leave" for an "extended vacation" that does not involve Iran. But his mother, reached by phone, said her son was in fact there.