



*Dr. Everet H. Beckner
Deputy Administrator for
Defense Programs*

The mission of the National Nuclear Security Administration's (NNSA) Office of Defense Programs (DP) is to achieve national security objectives through maintaining a safe, secure, and reliable nuclear weapons stockpile. This is accomplished through a variety of DP core functions, such as the Stockpile Stewardship Program (SSP). The SSP encompasses operations associated with maintaining, refurbishing, and dismantling warheads in the nuclear weapons stockpile. The SSP also includes nuclear test readiness and activities associated with the research, design, development, simulation, modeling, and non-nuclear testing of nuclear weapons for certification of safety, reliability, and performance.

DP customers include the NNSA Administrator, Department of Defense, Congress, various DOE mission area elements, external research and development agencies, industry, and academia.

DP also manages the Mutual Defense Agreements with the United Kingdom and France, focusing on collaborative activities in defense science areas such as high-energy density science and radiography.

I look to the Office of Counterintelligence to support DP personnel through their briefing and debriefing program. The information shared by the Counterintelligence Officers (CIOs) aids DP personnel in being aware of the types of activities that could pose a problem during foreign travel to DOE designated sensitive countries. Additionally, CIOs provide DP personnel information pertaining to hosting foreign nationals. Subsequently, DP personnel are more attuned to potential difficulties that can then be reported to the CIOs.

I have had occasions where CIOs have briefed me on issues of concern regarding my foreign travel along with briefings on foreign nationals visiting DP. The DP community understands the value of the support provided by CIOs and I recommend that all NNSA and DOE employees get to know their servicing Counterintelligence Office.

The Autonomous Pathogen Detection System (APDS)

By Jeff Morris, Lawrence Livermore National Laboratory

Shaped like a mailbox on wheels, it's been called a bioterrorism "smoke detector." It can be found in transportation hubs such as airports and subways, and it may be coming to a location near you.

Formally known as the Autonomous Pathogen Detection System, or APDS, this latest tool in the war on bioterrorism was developed at Lawrence Livermore National Laboratory to continuously sniff the air for airborne pathogens and toxins such as anthrax or plague.

The APDS is the modern day equivalent of the canaries miners took underground with them to test for deadly carbon dioxide gas. But this canary can test for numerous bacteria, viruses, and toxins simultaneously, report results every hour, and confirm positive samples as well as guard against false positive results by using two different tests. The fully automated system collects and prepares air samples around the clock, does the analysis, and interprets the results. It requires no servicing or human intervention for an entire week.

Unlike its feathered counterpart, when an APDS unit encounters something deadly in the air, that's when it begins singing, quietly. The APDS unit transmits a silent alert and sends detailed data to public health authorities, who can order evacuation and begin treatment of anyone exposed to toxic or biological agents. It is the latest in a series of biodefense detectors developed at DOE/NNSA national laboratories.

The manual predecessor to APDS, called BASIS (Biological Aerosol Sentry and Information System), was developed jointly by Los Ala-

(Continued on page 4)



The APDS operating near a ticketing counter at San Francisco International Airport. (The APDS unit is the dark gray box with the silver cylinder on top, located at the right side of the picture.)



IDENTITY THEFT – Protecting Yourself

By Deanna Austin, Office of Counterintelligence

In 2001 an estimated 500,000 – in 2002 an estimated 700,000 – in 2003 an estimated 10 million. These numbers reflect the fastest growing crime in America – identity theft. Frank Abagnale, a reformed thief, who details his criminal escapades in his book, “Catch Me If You Can,” states:

“Identity theft is one of those things you’re probably not very concerned about if it hasn’t happened to you. But...I don’t know of any crime that’s easier – and easier to get away with – than identity theft. Criminals realize it’s the simplest scam in the world. No one has to

see your face or know who you are. We live in a time when if you make it easy to steal from you, chances are someone will.”

Identity theft involves stealing names, Social Security numbers, credit card numbers typically for criminal purposes. However, according to the FBI, identity theft is rarely the sole objective of the crime but is almost always employed as a means to commit another crime. Identity thieves can open a new credit card account using your name, date of birth and SSN; establish phone or wireless service in your name; open a bank account and write bad checks; buy a car by taking out an auto loan in your name; or even file for bankruptcy to avoid paying debts incurred under your name. Some methods used to perpetrate these crimes include:

- “Dumpster diving” – rummaging through trash for personal information
- Fraudulently obtain credit reports by posing as a landlord or employer
- Stealing delivered mail; stealing a wallet or purse
- Completing a change of address form to divert mail
- Buying personal information from “inside” sources
- Using personal information shared on the internet

(Continued on page 3)

Official Web Site of the Federal Trade Commission
<http://www.consumer.gov/idtheft/>

The screenshot shows the website <http://www.consumer.gov/idtheft/>. The page features a navigation menu with links for **FILE A COMPLAINT**, **ORDER PUBLICATIONS**, and **PRIVACY POLICY**. A prominent red banner reads **ID THEFT HOME**. Below this, the text says: **Welcome to the Federal Trade Commission: Your National Resource for Identity Theft**. The main content area explains: "How can someone steal your identity? Identity theft occurs when someone uses your personal information such as your name, Social Security number, credit card number or other identifying information, without your permission to commit fraud or other crimes." It further states: "Identity theft is a serious crime. People whose identities have been stolen can spend months or years - and their hard-earned money - cleaning up the mess thieves have made of their good name and credit record. In the meantime, victims may lose job opportunities, be refused loans, education, housing or cars, or even get arrested for crimes they didn't commit." A sidebar on the left contains links for **ID THEFT HOME**, **CONSUMER INFORMATION**, **BUSINESS INFORMATION**, **LAW ENFORCEMENT**, **PRESS ROOM**, **ID THEFT STATISTICS**, and **EN ESPAÑOL**. A circular graphic with the word **THEFT** is also visible.

(Continued from page 2)

There are steps to reduce the risk of identity theft – remember, anything with an account number on it can potentially be used in identity theft.



- Avoid giving personal information over the phone unless you have initiated contact.
- Review banking, credit card and phone statements for unusual activity.
- Be wary of anyone calling or emailing to “confirm” personal information.
- Shred all credit, bank and other financial statements.
- Do not carry important documents such as your social security card, birth certificate, or passport except when absolutely necessary.
- Make a copy of the contents of your wallet or purse – both sides of each license, credit card, or identification card and keep in a secure place.
- Pay attention to billing cycles. A missing bill could mean a thief has changed your billing address; follow up with creditors if your bill does not arrive on time.
- Order a copy of your credit report from each of the three major credit-reporting agencies every year and review for accuracy.

WHAT DO YOU DO?

Equifax, (800) 525-6285
Experian, (888) 397-3742
TransUnion, (800) 680-7289

1. Contact the fraud department of any one of the three major credit bureaus and flag your file with a fraud alert.
2. Close accounts of concern.
3. File a police report
4. File a complaint with the Federal Trade Commission



OPSEC: An Overlooked CI Resource

By Ken Schiffer—Los Alamos National Laboratory

All DOE sites have an OPSEC (Operations Security) team tasked to conduct periodic OPSEC assessments of divisions and facilities in order to identify the possible, inadvertent loss or compromise of sensitive or classified information. However, the potential value of OPSEC to CI is often overlooked.

In the science and weapons laboratories, cutting edge technologies are being developed or researched; identifying and protecting these technologies is part of CI’s mandate to prevent the loss of information or technologies which would damage national security. Identifying the specific countries targeting a specific technology is a continual process. The task of identifying the “loss paths” or ways that information can be compromised (e.g. through exchange with foreign nationals, during foreign travel, conferences, carelessness, etc.), and developing methods to prevent loss is important to the CI mission. OPSEC can assist in all these areas.

OPSEC’s mission is to answer five basic questions:

- What information or resources should be protected?
- Who wants this information?
- What is the consequence if it is compromised?
- How can it be compromised?
- What measures can be instituted to prevent compromise?

At Los Alamos National Laboratory (LANL) the OPSEC team is part of the CI program and provides critical assistance. OPSEC identifies what technologies are being worked; then determines which of those technologies should be protected. This Critical Program Information or CPI is fed into a web site available to all CI staff and into a technology database which can crosswalk the information that should be protected against the collection requirements of specific countries. OPSEC is also responsible for the CI/CT awareness program at LANL and utilizes the OPSEC Working Group comprised of representatives from all laboratory offices and divisions, to provide timely and relevant CI/CT information directly to management and workers.

While it is recognized that LANL is unique in including OPSEC as a part of its CI office, for this site it has proven to be an effective resource in the Laboratory’s CI mission and has potential value to other sites as well.



PATHOMICS

By Jeff Morris, Lawrence Livermore National Laboratory

An alarm sounds in a subway's Automated Pathogen Detection System. Health officials know that people have been exposed to a deadly bioterrorist agent. But who has been exposed and needs to be treated? Must people develop symptoms before diagnosis occurs and treatment begins? By then, it may be too late, and exposure may have spread.

A new approach to disease detection called "pathomics" is underway at Lawrence Livermore National Laboratory. Its aim is to diagnose infection well before symptoms appear.

Pathomics is based on the premise that changes in protein levels and other molecules occur in the blood when someone is getting sick, but hasn't yet begun to show symptoms.

The potential uses of this new science are far broader than providing early diagnosis of disease in individuals. Pathomics could indicate mass exposure to bioterrorist agents such as plague and anthrax as well as to bioengineered agents and to new diseases.

The underlying rationale of pathomics research is to move from the discovery of a disease's "signature" to its application in the country's bio-defense system. LLNL and Los Alamos National Laboratory used a similar rationale to apply scientific discovery to develop the Biological Aerosol Sentry and Information System (BASIS).

BASIS technologies focus on detecting deadly biological agents in the air. BASIS was deployed during the 2002 Winter Olympics. Its technologies and architecture are the foundation of the national BioWatch detection system, which is used in approximately 30 U.S. cities.

Pathomics will complement Biowatch. While Biowatch is designed to detect releases, pathomics can be used to determine who has been exposed to deadly bio-agents. Pathomics' developers believe the combination of Biowatch and pathomics will increase the nation's ability to detect and respond to bioterrorist threats.

A 15-person research team at Livermore is involved in the pathomics project, which began in April 2003. Plans are to continue it for another year and a half. LLNL researchers are working in collaboration with the University of New Mexico Health Sciences Center and the Center for Biomedical Inventions at The University of Texas Southwestern Medical School at Dallas.

(Continued from page 1)

mos and Lawrence Livermore National laboratories. That system was modified to become BioWatch, the Department of Homeland Security's biological urban monitoring program. A related laboratory instrument, the Handheld Advanced Nucleic Acid Analyzer (HANAA), was first tested successfully at LLNL in September 1997.

Successful partnering with private industry has been a key factor in the rapid advancement and deployment of biodefense instruments such as these. The APDS technology has been licensed and is currently undergoing commercialization.

ARTICLE SUBMISSIONS AND READER FEEDBACK WELCOME!

Counterintelligence Quarterly:
Reporting on the nexus between quality
science, technology and
counterintelligence

Published by:

U.S. Department of Energy
Office of Counterintelligence and
Office of Defense Nuclear
Counterintelligence
1000 Independence Avenue, SW
Washington, DC 20585

Managing Editor:

Deanna Austin
Phone (202) 586-0432
Fax (202) 586-0551
email: ci.quarterly@cn.doe.gov

LOCAL COUNTERINTELLIGENCE OFFICE CONTACT INFORMATION

Office of Counterintelligence
Richland Regional Office
Contact us: By Email:
^OCINWREGION
OCINWREGION@RL.GOV

By Telephone: 373-1865

Visit our website at:
<http://www.hanford.gov/oci/index.cfm>