Cybersecurity in the Year 2000:
Not Just for Systems Administrators Anymore

Panel Chair

Richard Shullaw, Security Manager
Office of Child Support Enforcement
Administration for Children and Families
Department of Health and Human Services

Panel Membership

Danny Markley, Senior Security Analyst
Office of Child Support Enforcement
Administration for Children and Families
Department of Health and Human Services

Robyn Large, Training Course Developer
The Center for Support of Families

Marianne Swanson, Computer Specialist
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

Panelists' Position Statements

Richard K. Shullaw
Federal Office of Child Support Enforcement

Overview of Panel Presentations

Not so long ago, few of us would know what cybersecurity involved. We knew in a vague sense that it involved computers, and felt that it was best left to those who were most familiar with those devices: system administrators. We now understand that cybersecurity is a key issue that can affect our daily lives. Not a day goes by without a news or television story involving some aspect of cybersecurity. Major commercial web sites are rendered unusable because of denial of service attacks. Government sites are hacked and defaced. Viruses spread within hours to infect hundreds of thousands of computers, causing e-mail and other information systems to grind to a halt.

Along with the increasing awareness of cybersecurity is concern about privacy of personal information. Michael Saylor, the owner and founder of Microstrategy, talked in a recent interview about the ability of data extraction systems to put together profiles on individual users. He said that these will ensure that users are told of the books they like to read, and the entertainment they enjoy based entirely on previous buying patterns. Opinions on the desirability of this capability vary. Some view it as a simplification of life. Others view it with alarm as an invasion of privacy.

Our panel will look at the issues of cybersecurity as they affect child support enforcement programs. At the Federal and State levels of government, this program provides substantial benefits to a highly vulnerable group: single parents and their children. Sophisticated national information systems support State efforts to increase the amount of child support collected. In 1999, over $15 billion was collected in child support, a 100% increase over the amount collected in 1992. $1.3 billion was collected through the Federal Tax Offset program in 1999, a $250 million increase over collections in 1998. Through data exchange with the Department of State, a program has been instituted to deny passports to those who owe more than $5,000 in back child support. Arrangements have been made with financial institutions so that States can identify assets of those who owe child support for freeze and seize actions. Because of the scope of the data we work with, and the sensitivity of the information we handle, we have taken active steps to ensure the privacy and security of the data.

I will lead off the discussion with a brief description of the scope of the databases we operate. Danny Markley will follow with a discussion of the security concerns OCSE faced, and the actions taken to address those concerns. Robyn Large will then describe the multi-faceted training program we have developed to get the security message out to our state and other partners. Finally, Marianne Swanson, who has provided invaluable support to OCSE in developing its security capabilities, will provide an overview of what events and government activities will affect near-term cybersecurity initiatives.

Richard K. Shullaw
Federal Office of Child Support Enforcement

The Federal Parent Locator Service (FPLS) Database

The genesis of the current FPLS database is the Welfare Reform Act of 1996 (also known as the Personal Responsibility and Work Opportunity Reconciliation Act (PRWORA). The elimination of the old Aid for Families and Dependent Children (AFDC) program required establishment of new resources at the Federal and State levels. These were designed to assist State Child Support Enforcement Agencies in: establishing paternity; establishing, setting the amount of, or modifying child support obligations; and enforcing child support obligations.

States were required to establish State Directories of New Hires (SDNH), State Case Registries (SCR). State data was consolidated in an expanded Federal Parent Locator Service (FPLS), which is made up of two components:

- The National Directory of New Hires (NDNH), which contains new hire, quarterly wage, and unemployment insurance payment information on all wage earners, including Federal employees; and
- The Federal Case Registry of Child Support Orders (FCR), which contains a national registry of all child support cases.

Automatic matches are made between the FCR and NDNH to supply States with current and highly usable information on the location and employment of non-custodial parents involved in child support. No longer is a move by a non-custodial parent a guarantee of avoiding child support obligations.

In addition to the FPLS database, OCSE operates the Tax Refund Offset System (TROS). State child support enforcement agencies supply data on delinquent obligors to OCSE. That information is matched against tax refund information from the IRS. If an obligor is owed a refund, delinquent child support is deducted from the refund and sent to the custodial parent. A further use of the delinquent obligor data is to provide names to the Department of State. If an obligor owes child support and applies for a passport, the application is denied until the obligation is satisfied. Finally, this data is also used to match against account information of multi-state financial institutions. The State handling the child support case is notified of the match so that freeze and seize actions can be taken.

The sheer size of these databases is impressive. As of April 2000, the NDNH contained

- 134 million new hire records
- 1.2 billion quarterly wage records and
- 56 million unemployment insurance records.

For the same time period (April 2000), the FCR contained over 13.5 million cases and 27 million participants. The Multi-State Financial Institution Data Match (MSFIDM) involves agreements

with over 3,000 financial institutions (banks, savings and loans, brokerage houses, and credit unions). MSFIDM, which became operational in August 1999, has to date matched more than 879,000 obligors with accounts that can be pursued by state child support agencies.

The fact that the NDNH contains wage information on every wage earner, with the vast majority not being involved in any child support issues, has raised concerns among privacy advocates. An article last year in the Washington Post on the NDNH was titled "Uncle Sam has all your numbers; huge net for deadbeat dads catches privacy criticism." The article provided a concise summary of the pros and cons involved with the NDNH.

OCSE has taken a pro-active approach to ensuring the security of the data and the legitimate privacy concerns of individuals. Danny Markley will now describe steps that have and are being taken in this area.

Danny L. Markley
Federal Office of Child Support Enforcement

The Child Support Program has undergone many changes due to the implementation of Welfare Reform in 1996. Welfare Reform mandated that the federal Office of Child Support Enforcement (OCSE) create a database to assist States in the location of individuals involved in child support cases. Thus, the Federal Parent Locator Service (FPLS) was born. The development of such a massive database, containing information on practically every person in the United States, raised security concerns about privacy issues, safeguarding of sensitive data, personal security and physical security.

Due to these concerns, the national spotlight was quickly focused on the security of the FPLS database. During the first year of operation, OCSE received inquiries from OMB, Congress and many members of the media. Also during the first year of operation, a number of government agencies such as SSA, IRS, and GAO conducted audits to evaluate the system of safeguards in place. The audits performed by the IRS are of special importance. Because FPLS handles tax data, we must ensure that IRS security requirements are met in addition to OCSE requirements.

The OCSE Security Team developed a security program focusing on areas of personal, physical and computer security, to promote awareness, training, internal controls, and a system of safeguards to protect the data. The focus of the program was to make sure that staff working with OCSE data was aware of its sensitivity, would handle it accordingly, and would bring to management any problems they saw with the way data was handled.

One of the many priorities involved implementing a system of security requirements at OCSE and the SSA's National Computer Center (NCC) Facility. This process involved restricting employee and visitor access to certain areas of the facilities, restricting and closely monitoring system access, and monitoring and controlling the movement of data through a number of processing stages.

Robyn Large
The Center for Support of Families

It used to be when you mentioned the word security, the common reaction was “it is someone else’s job" or you were faced with blank stares and bored faces. Security guards and blue suits often flashed through your audience's minds. Not any more. Technology is revolutionizing the way we do business and has changed the rules of security and privacy.

In the security courses that have been developed for the child support program, we found it critical to make security a personal issue to drive home the importance of protecting the vast amount of information available to the child support worker. The sensitivity of this information brings serious security implications to day-to-day operations.

To make the training relevant we discuss threats that impact each one of us personally and then tie this into their workplace. The course covers such issues as:

- *Identity Theft* which is reaching epidemic proportions;
- *Cyber-hacking* which is continually front-page news; and
- *Virus threats,* which appear almost daily.

We also discuss that over 1 million people are hurt in the workplace annually due to workplace violence.

The first course developed was the Child Support Enforcement Program—Securing the Future: Training of Trainers (TOT) Course. This six-hour train-the-trainer course is designed to prepare trainers to deliver the security course to child support personnel. The course focuses on raising security awareness and the need to make security a priority in your personal life, the child support program, and the office. This course focuses on the changing world of technology and its impact on the job.

The next course is the Child Support Enforcement Program—Securing the Future: A Manager’s Perspective. This course was developed for managers in child support offices. The four-hour course is designed to focus on security from the manager’s perspective. Managers will learn the critical role they play in ensuring security of information, personnel, and other assets, as well as the need for both security and disaster recovery plans. The course will provide managers with an assessment of where they are in security preparedness and provide helpful tools to design and implement a comprehensive, successful security plan.

In both of the courses we use The Child Support Enforcement Program—Securing the Future Video produced by OCSE. This 13-minute video draws attention to the data and physical security issues in child support enforcement. The video uses real life scenarios and interviews to demonstrate that the careless use of, or unauthorized access to, the data could result in physical harm to the families we serve, and that the data could be used in criminal activities such as fraud and identity theft. The video discusses how protecting the data and ensuring the physical safety of our child support offices is essential to the continuation of our much-needed services.

We have also developed an Assessment Tool that is designed to help Child Support managers assess their agency's strengths and weaknesses with respect to security issues. The tool should be used to evaluate each area of security and provides an assessment of where their office stands today. There are suggestions and helpful information that will assist them in enhancing their security capabilities in each area that is evaluated.

The design of the material and the delivery of the course are very important. We have developed a course design that includes each PowerPoint slide on the same page with the text. This allows the participant to follow along with the trainer. A note-taking page is on the opposite side for their own use as well. These courses are developed with the intent to be delivered to the child support worker and child support managers. It is most effective when you can deliver the message directly to the key personnel involved.

We have found that the most important and powerful element that has made this training successful is tying the message to personal experiences. Once you have your audiences' attention, their minds will be thinking about how they can be more proactive in dealing with security and confidentiality issues in their daily lives. You can then turn the focus toward similar issues that exist in the workplace. The goal is to raise awareness in both areas. If we are more cautious and thoughtful about these issues at home, we will tend to act in the same way at the workplace.

Marianne Swanson
NIST

The Information Technology (IT) field continues to evolve at a rapid rate. New guidance, new requirements, and new and proposed legislation are nipping at the heels of technology in the IT revolution race. From the security implementers' perspective, it is hard to keep up on all the security, privacy, and accessibility issues. It is even harder to secure IT resources when new software vulnerabilities are routinely found and exploited. However, as we have seen in the recent news, the result of not staying current can be disastrous.

The government has begun a number of initiatives to reduce vulnerability to cyber attacks. Presidential Decision Directive (PDD) 63, issued in May 1998 by President Clinton, mandated that Federal Departments and Agencies assess the vulnerability of critical national infrastructures to cyber attack. The directive places special emphasis on protecting the government's own assets from cyber attack and the need to take action to correct any deficiencies that are found. In January of this year, the White House issued the National Plan for Information Systems Protection. The plan provides an initial road map and a list of actions required from the government to enhance its cyber security.

Under PDD 63 and the National Plan, NIST and the Office of Management and Budget have been assigned major responsibilities. These include the conduct of independent analyses and testing to determine agency vulnerabilities.

To obtain a current picture of IT security at the U.S. federal level, a brief synopsis will be provided of the U.S. federal IT security requirements, how to obtain current information, and several IT security projects that the National Institute of Standards and Technology is involved with.