



## Preventing Insider Fraud at Government Agencies

### The Insider Threat

Government agencies around the world are facing a growing threat to their information assets from within – their own management and employees. Fraud and information leakage committed by knowledgeable and capable employees who utilize their knowledge of IT systems and controls to manipulate internal systems can cause much greater damage than third parties. The various inside fraudulent activities include manipulating financial transactions, misappropriating assets, selling citizens private data, and others. Beyond fraud, there could also be noncompliant transactions in the form of errors or intentional overrides.

### The Audit Trail Challenge

FISMA (Federal Information Security Management Act), HIPAA and other regulations require government agencies to maintain detailed audit trails of access to sensitive data in their information systems. This requirement is challenging, especially for organizations that rely on heterogeneous platforms including legacy systems as these systems typically do not provide sufficient application access logging. Developing such a mechanism, involves tremendous effort and cost, potentially altering thousands of programs. Mechanisms that track changes to corporate databases are not sufficient, as they typically track update transactions but do not capture critical "read-only" access to data. In addition database monitoring solutions typically lack the ability to capture the actual user-id who accessed the information, as most applications use generic user-id when accessing the database.

### The Intellinx Cross-Platform Solution for Internal Fraud Detection

Intellinx presents a breakthrough in insider threat detection and prevention. It provides a first-of-its-kind cross-platform surveillance system for unparalleled visibility of end-user activity in corporate applications across the enterprise. The Intellinx Solution provides a critical infrastructure for combating internal fraud and information leakage, making authorized users accountable for their actions. Intellinx is the only product on the market today that provides the following:

- **Unparalleled Visibility to End-User Activity** - Complete visibility into end-user activity is provided with visual replay of every screen and keystroke and client/server message in every application across all major platforms. All actions are visible, including update and read-only actions. All types of end-users are tracked including privileged end-users such as System Administrators and Database Administrators that may pose a higher risk as they have higher authorization levels.
- **Complete Audit Trail** - Intellinx records the full user activity 24x7, not just events detected as suspicious in real time. This is crucial for making end-users accountable for their actions. Regardless of whether appropriate rules are in place at the time of an event, post-event replay enables forensic investigation at a later time.
- **Cross Platform Search including Legacy** - Intellinx provides a unique solution for tracking user activity across all major platforms including mainframe, iSeries, Web, Client/Server and more. It allows you to search for any specific value displayed on any user screen across multiple platforms from one simple query screen. The Intellinx rules track cross-platform business processes. For example, a business process tracked by Intellinx may start on iSeries, continue in a client-server application and end on the web.
- **User Behavior Profiling at the Application Level** - Intellinx is the only solution on the market that analyzes the user activity at the application screen level (not at the network or database level). Intellinx rules track all user keystrokes and the flow of screens accessed by the user, detecting the relevant business process including each field value accessed or updated. This information is correlated in real-time with the activity of other end-users, with previous activity and other types of information generating alerts on suspicious behavior near real-time.

### The Challenges

Following are several examples:

#### Tax Refund Fraud

A Department of Revenue employee changes a taxpayer's bank account number, processes a refund payment and then changes the bank account number back. How can you prevent it?

#### Leakage of Sensitive Information

A State Police employee leaks information on a homicide case investigation to one of the suspects. How can you stop it in time?

#### Privileged IT User plants a Logical Bomb

A disgruntled State Agency programmer plants malicious code which sporadically deletes taxpayer accounts. To cover his traces he compiles the program, removes the malicious code from the program source, then saves the clean source. How do you reveal what he did?

#### Segregation of Duties

A change in beneficiary status in the Social Security Administration requires manager approval. A clerk tries to enter his manager's password but fails and the transaction is not completed. How do you find out?

#### Leakage of Health Information of Celebrities

A Social Security Administration employee browses through sensitive health information of celebrities and leaks it to the press, which creates a scandal. How do you find who did it?

