



Critical Incident Response Group (CIRG)

The Situation

Congress mandated the creation of the Critical Incident Response Group (CIRG) to operate critical incident response within the Washington Capital region. CIRG is operated by FBI Agency staff and includes users from several other federal agency members. Their objectives during an “incident” are 1) maintain the security and safety of senior government officials and 2) contain or minimize the adverse effect of the incident. Considering the potential devastation such an incident would present to national security, communications are critical. Practice exercises are initially run quarterly to develop and maintain optimal operational capability.

The Communications Challenge

Typical incident management procedures use two key paper-based tools:

- An Event Checklist of several hundred action items updated via a PC on a spreadsheet in a Sensitive Compartmented Information Facility (SCIF), then printed out and faxed to SCIFs in other CIRG members’ dispersed locations. This process can repeat at a fixed window of time, usually every 15 minutes for up to 48 hours depending on the exercise duration.
- A comprehensive Activity Log updated in real-time to reflect all incident activity in meticulous detail; updates include action requests, decision-making factors, completed activities, etc.

Despite the critical nature of CIRG communications in these scenarios, the tools’ manual update process exhibits multiple points of vulnerability and potential process breakdown.

“I want this in my office, on my PC.”

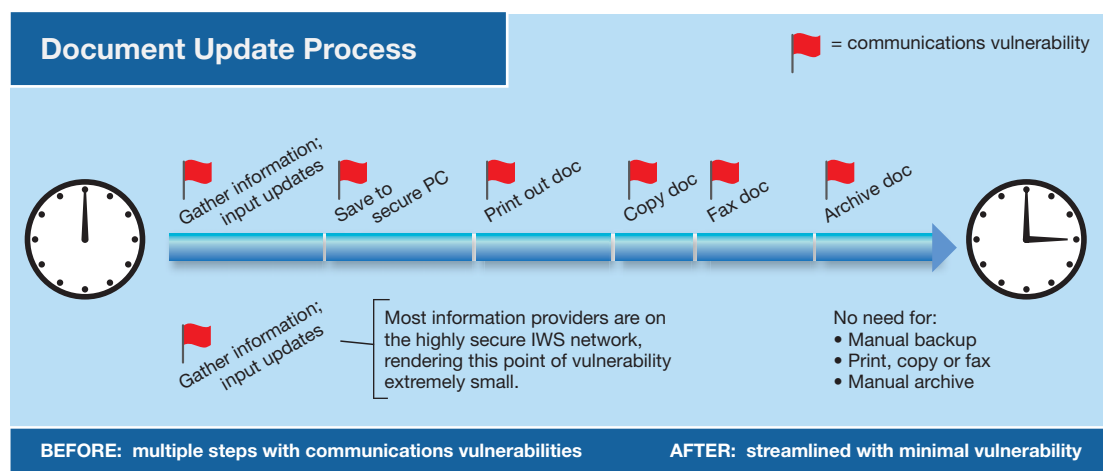
FBI SENIOR STAFF,
COMMENTING ON EZENIA!
INFOWORKSPACE.

Process Step	Point of Vulnerability
A “Document Keeper” in a SCIF with a secure PC inputs updates from various sources, including phone, fax, text message — even handwritten notes!	<ul style="list-style-type: none"> • Critical information can be delayed and must “beat the clock” to be transmitted as quickly as possible • Illegible handwriting or a garbled message can result in an update error
The DK saves the updates on the secure PC	<ul style="list-style-type: none"> • Risk of single point of hardware/software failure • Subject to human error — accidental document erase during a shift change, agent training or simply human fatigue
The DK prints out the updated document	<ul style="list-style-type: none"> • Lost time while waiting for document to print • Subject to printer error — no paper, paper jam, low ink
The DK makes several copies of the printout	<ul style="list-style-type: none"> • Lost time while waiting for copies to generate • Subject to copy machine error — no paper, paper jam, low ink
The DK faxes the document to each agency location that is required to receive the document on a set schedule, sometimes every 15 minutes	<ul style="list-style-type: none"> • Lost time waiting for fax dial tone, receiving fax to pick up then transmit multiple pages • Subject to receiving fax error — no paper, paper jam, low ink • Someone must officially “receive” the fax at the other end in a secure room
The DK archives the document and the cycle renews	<ul style="list-style-type: none"> • Paper-based archive subject to human error — misfiling • Computer-based archive subject to single point of failure

The InfoWorkspace Solution

CIRG initially reached out to Ezenia! for **Text Chat** capability to supplement the existing manual Checklist and Action Log methodology. However, once Ezenia! learned of CIRG’s extensive information-sharing requirements, we designed a new product feature — **EZinFORM** — to address those requirements in a customized manner. Ezenia! presented EZinFORM in concept and CIRG immediately realized its tremendous potential as a comprehensive and secure solution.

Ezenia! quickly engineered and incorporated EZinFORM into the IWS COTS product, providing a document management template to replace the paper-based tools. Leveraging IWS’s extensive core feature set in conjunction with the highest levels of security compliance, easy administration, and active server backup, CIRG was able to create a protocol of operations which streamlined their update process and eliminated nearly all of their communications vulnerabilities.



Increased practice frequency, capability and efficiency

The InfoWorkspace Solution in Action

EZinFORM can display both Checklist and Action Logs instantly to numerous CIRG members in disparate locations. **Intuitive GUI** displaying buildings, floors and rooms, permits multiple CIRG agents to simultaneously and securely view the forms and support the update process. Ezenia! also created an EZinForm **View Only** rights option allowing the **Security Administrator** to restrict viewers’ editing privileges while maintaining their secure viewing status. For additional security, Administrative structure permits defined user permissions at multiple granular levels.

CIRG also chose to leverage IWS’s **Instant Messaging Text Chat** for users to enjoy the freedom to communicate privately and even institute a **Room Lock** for one-on-one briefings. This capability is most helpful in scheduling exercises, reviewing new concepts and in assessing “after- action” reports for process optimization.

The Impact

CIRG **increased their pilot exercise efficiency significantly**, from a once per quarter paper drill to as often as once per month paperless. This additional “practice time” also allows CIRG to study more diverse scenarios, enhance their response to a potential threat, and focus on their critical mission of national security.