R

Reinforcing Security at the FBI

Gregory F. Treverton, Richard Darilek, Mark Gabriele, Martin Libicki, William (Skip) Williams

MR-1687.0-PSJ

February 2003

Prepared for the Security Division of the Federal Bureau of Investigation

RAND Institute for Public Safety & Justice

The purpose of the dot-zero MR is to minimize delays in getting final reports and other deliverables to clients. Dot-zero MRs are formally reviewed but generally not edited. It is expected that dot-zero MRs will become final MRs.

PREFACE

This assessment was requested of RAND by the Security Division (SD) of the Federal Bureau of Investigation (FBI). Its point of departure was the Robert Hanssen spy case and the subsequent blue-ribbon panel that investigated that case. Hanssen was an FBI Supervisory Special Agent who spied for the Soviet Union and Russia for twenty-two years; his case was, in the language of the panel's report, "possibly the worst intelligence disaster in U.S. history." The panel was chaired by former FBI (and CIA) Director, Judge William Webster, and its report, *A Review of FBI Security Programs*, Commission for Review of FBI Security Programs, Washington, March 2002, is available on the web at http://www.usdoj.gov/05publications/websterreport.pdf (Hereinafter referred to as the "Webster Commission" or "Webster report.")

The RAND assessment was a three-month effort. It comprised a review of the Webster Commission report and its classified appendices, along with relevant plans and other materials from the SD. The RAND team conducted several score of interviews with FBI officials, throughout the organization, and it visited several of the FBI's Field Offices. The assessment's purpose was not to attempt to redo the Webster Commission. There was neither need nor time to do that task.

Rather, RAND was asked to look again at the Webster Commission's recommendations in light of September 11 and the war against terrorism (the Webster Commission largely completed its work before September 11, though it was published afterward). And it was asked, more generally, to assess the progress of building a security program at the FBI that would sharply reduce the risk of another catastrophic failure of the sort represented by Hanssen. The final part of that task - judging the adequacy of timelines and resources for the security program - could be accomplished only in part. Given the number of decisions bearing on that program that are yet to be made, with plans yet to be developed,

this assessment concludes with general observations about time and resource isgues.

This project was done within RAND Public Safety and Justice, which conducts research into a wide variety of aspects of crime, violence, and public safety, including illegal immigration and border control; fire safety, evacuation, and rescue; food processing and safety; domestic counter-terrorism, terrorism preparedness, and threat and vulnerability management; and emergency first-response capability. Much of the research is conducted through three centers - the Criminal Justice Center, the Drug Policy Research Center and the Public Safety Center.

CONTENTS

SUMMARY

The FBI security program has made notable progress in the last two years in moving forward with the agenda set out by the Webster Commission. While responding to September 11 has dominated everything the Bureau has done, the security program is being implemented with dedication and enthusiasm. Most importantly, there appears to be a senior leadership commitment to make security a key concern of FBI operations and support programs. In addition, the newly created Security Division (SD) team is stepping in the right direction to implement comprehensive reforms that place security within the fabric of FBI culture.

The purpose of this independent assessment is not to redo the Webster Commission - a task for which there was neither need nor time. Rather RAND was charged with asking how the events of September 11 and the revamping of the FBI mission in light of those events have changed the task of security, and to provide an independent assessment of the progress the FBI has made in reinforcing its security.

Most of what has been accomplished can be attributed to the security structure provided by senior leadership as a consequence of creating a Security Division. That creation brought a cadre of security-minded officials drawn, in many cases, from agencies and offices within the intelligence community and dedicated to a "never again" set of goals. They brought rigor and a process for meeting internal and external security tasks. The new structure centered security policy at an appropriate senior level, helping with implementation and providing the Director with a senior advisor on security matters.

For all the progress, though, it is still early in the security policy process, and the obstacles ahead are formidable. As we note in several places in this report, and as the FBI Security Program Plan (SPP) clearly acknowledges, many policy decisions of major importance

remain to be made. Thus, it is too early to make judgments about the adequacy of future resource commitments to security; they can be judged when major policy decisions and more concrete implementing plans are in place.

In that vein, the recent program/project management initiatives seem on the right track. Engaging MITRE, a top flight systems consultant, and creating a team to look at project and program management should provide more reach and coherence while taking some of the pressure off already over-burdened senior managers. Any efforts to increase buy-in by section and unit chiefs is welcome, as are any efforts to sort contemplated actions into projects and to begin to make priorities among those projects. The next steps - to look at what is missing, and to evaluate budgets in light of priorities - should provide the wherewithal for a probing assessment of resources and timelines.

For instance, the SPP specifies five years as the goal for ''the FBI transitioning into an organization in which security is considered a core function and is recognized for its value-added to operations and personal safety. (p. 19)'' On its face, five years seems like a reasonable schedule to accomplish all that has to be accomplished, assuming the resources are available. But, again, a more useful assessment cannot be made without knowing more of the specific policies and plans called for in the SPP but not yet in place.

The metrics set out in the SPP (pages 39-40) would be a useful starting place for a resource adequacy assessment if there were resource estimates stacked up against them. Now, they are about getting SD organized and staffed, and thus are aimed at a high-level audience. They are only for FY 2003 so they would obviously have to be extended across the entire five-year plan, which also seems about the right horizon for resource planning. The metrics only call for ''20 percent'' of the ''security risk analysis capability in the final Security Division structure'' to be operational in that year, which raises the question of whether it might not be possible to do better.

One thing that does seem missing is any plan for a serious ''Red Team'' effort to try to break through existing security. This should be a part of the plan, separately organized and funded. Related to this, the fourth of the ''priority performance gaps'' noted on page 15 was ''Security programs are not adequately addressed to determine the effectiveness of targeted programs.'' This point is downplayed it the rest of the report, mentioned only in passing several other places. We would recommend that a major specific part of the SPP be a plan for policy effectiveness assessment, and the resources to do it.

The most important set of decision in process and yet to be made concerns Trilogy, the Bureau's very expensive new information system. The security structure of Trilogy will affect how the Bureau approaches its work processes - how both criminal case and national security-derived information are shared. The longer decisions bearing on security policy are put off, the more likely it is that Trilogy will not adequately embody required security qualities.

SD has moved quickly, with contractor help, to oversee the critical decisions about Trilogy. Yet while these decisions critically affect security, the interests at stake, in Trilogy and other matters, run well beyond security to include, especially, the interests of agents in the field who are trying to get the job done. They thus require attention at the highest levels of the FBI, including the senior leadership in each of the FBI Field Offices and major supporting organizations.

Reinforcing security at the Bureau amounts to a major change in organizational culture, one that is occurring at the same time as the Bureau is reshaping its mission. The change is visible; Field Offices that a year ago let security reinvestigations lag as low priority business now call in advance to get next month's roster of those who are up for reinvestigation. We also found added emphasis in getting security input early when offices are contemplating moving or doing construction. There is a greater awareness that security, like other enablers such as

safety, should be intrinsic to all operations and support, part of FBI best practices and agent tradecraft.

However, security cannot be imposed from outside the Bureau. To be effective, it must come from within and be pushed by internal groups with operational credibility. Security issues need proponents within the training and operational culture of the FBI. While there is a security presence during initial agent training, it is modest, and while opportunities to discuss security issues with mid-career personnel are increasing, they remain few. Without more opportunities for educating agents and support personnel, the process for balancing security with operational necessity will lack the operational pushback that is needed.

Future FBI security efforts need to focus on:

·Professionalizing the Bureau's security operations - as well as the larger information technology (IT) structure in which they are embedded. Professionalizing security is very much a part of the current program. Given the relatively low priority of security, work in the area has not been a profession. It is, for most at headquarters especially, a collateral duty, not a primary one. The duties of security officers have been mostly administrative, revolving around personnel security paperwork. Security officers have not generally been asked to be, and are not, proactive. The intention to create a cadre of security professionals, including special agents but also non-agents, surely is the right one. The questions here are resources and the role of agents in an agent-dominated culture.

·Institutionalizing "need-to-know" - that is, the principle that particular sensitive and classified information will not be available to those whose work does not require them to see it, even if they have the appropriate clearances. For reasons deeply rooted in the Bureau culture and in law enforcement, "need to know" was not really applied, and in many ways was not really thought through. Robert Hanssen continued to have access to information when he no longer had a valid need to know.

Likewise, local law enforcement personnel detailed to a Bureau-hosted Joint Terrorism Task Force probably do not have a need-to-know when it comes to criminal corruption cases. The issues here are how to institutionalize need-to-know while impeding as little as possible the free internal flow of information that has been the hallmark of the Bureau's law enforcement culture.

·Making threat assessments more systematic. At present, threat assessments seem to be made in a mostly *ad hoc* manner. How should the threat be conceived, when non-state actors - ranging from organized crime, through rich swindlers, to terrorists - are now more threatening? In the investigations area, for instance, there seems the most concern about new hires, especially translators, born abroad and now in mid-life. That seems fair enough, but whence does it derive? Some mechanism for more systematic threat assessment seems necessary, both to guide the security program generally and with respect to specific systems.

·Recasting squad and support group work processes within the new security environment. Current work processes hinge on opening a case in response to a crime. A case provides the context for gathering information, assigning investigation tasks, and even assigning need-to-know. Yet, as the Bureau's mission shifts from law enforcement toward prevention, from reaction toward pro-action, the case model may not support all FBI missions. Terrorist groups, for instance, might only commit a crime at the end of a long chain of activity, so working proactively against them means looking at predictive criminal behaviors within an information-intensive environment. The security foundation required will be different from that for case-driven law enforcement.

·Harmonizing new technology to work smarter with technical security concerns about information and personnel. Careless cell phone practice, for example, not only puts at risk operational information but may also allow a technologically aware adversary to track a user's position. While today this may be mostly a risk overseas, the risk of compromising

a domestic operation is present. At one level, this means that security must balance risk with deliberate process. At another level, it means that the technical security input must have credibility with core work groups lest those groups ignore or work around security directives. This may also require the Bureau security effort to invest in research to best leverage technology within an operational context, and it will dictate a renewed commitment to technical security education and training at the entry and in-service levels.

Revising the operating manuals (Manual of Investigative Operations and Guidelines, MIOG and, Manual of Administrative Operations and Procedures, MAOP). This would seem minor but has more than minor implications. Because major parts of the manuals are so out of date, when the Field Offices (FOs) are inspected, they get penalized for security violations that no longer matter much, while more serious concerns go unnoticed. The poor focus trivializes what should be an important process. It also penalizes the security officers while letting supervisory special agents off the hook.

There are no absolute guarantees in the security business. And rightly so, for security is not *the* business for the FBI or most other organizations. Instead, the overarching security goal, in the language of FBI security managers, is to reduce the time from "defection to detection" and to do so with as little cost to the efficiency of ongoing operations as possible.[1]

[1] This adage, a catchy one, is widely used as shorthand. To be sure, it is not a complete description of the goal, which would also include, for instance, limiting a possible traitor's access to sensitive information during the period between defection and positive detection.

ACKNOWLEDGMENTS

We are grateful to our RAND colleagues, Robert Anderson, Kevin O'Connell and James Quinlivan, for their insightful comments during the process of this project, as well as those of Jack Riley, who directs RAND Public Safety and Justice. It is the nature of assessments like this one to focus on what is still wrong, not on what has been made right, on what is yet to be done, not what has been accomplished. However, much has been accomplished, and we want to acknowledge our colleagues at the FBI, whose help in producing this report we appreciate and whose dedication as public servants we admire.

GLOSSARY

Symbol	Definition
ACS	Automated Case Support
AIU	Analytic Integration Unit (SD)
AIU	Asset & Information Unit (CID)
ASD	Administrative Services Division
BAEU	Bureau Applicant Employment Unit
BICS	Background Investigation Contract Service
C & A	Certification & Accreditation
CD	Counterintelligence Division
CDAR	Case Document Access Report
CID	Criminal Investigative Division
CIMS	Criminal Informant Management Division
CT	Counterterrorism
CTD	Counterterrorism Division
DISCO	Defense Investigative Security Clearance Office.
DoJ	Department of Justice
ESOC	Enterprise Security Operations Center
FBI	Federal Bureau of Investigations
FBINet	FBI Intranet
FISA	Foreign Intelligence & Surveillance Act
FO	Field Office
HCS	Human Intelligence Control System
HUMINT	Human Intelligence
IA	Information Assurance
IRD	Information Resources Division
IM	Investigative Mainframe
IS	Information Systems
IT	Information Technology
ITD	Investigative Technologies Division
JTF	Joint Task Force
LEGAT	Legal Attaché'
MAOP	Manual of Administrative Operations & Procedures
MIOG	Manual of Investigative Operations & Guidelines
NYFO	New York Field Office
PDA	Personal Digital Assistants
PENTTBOMB	September 11th Investigation

PENTTBOMB	FBI Investigations into September 11th attacks
PKI	Public Key Infrastructure
PSI	Personnel Security Interview
PSP	Personnel Security Polygraph
SAC	Special Agent in Charge
SCIF	Sensitive Compartmentalized Information Facility
SD	Security Division
SI	Security Investigator
SPP	Security Program Plan
TTA	Technically-Trained Agent
UA	User Application
VCF	Virtual Case File
VPN	Virtual Private Network
WFO	Washington Field Office
Wi-Fi	Wireless fidelity, popular term for high-frequency wireless LAN.

I. REINFORCING SECURITY AT THE FBI

PURPOSE OF THE ASSESSMENT

The purpose of this independent assessment is not to redo the Webster Commission - a task for which there was neither need nor time. Rather RAND was charged with asking how the events of September 11 and the revamping of the FBI mission in light of those events have changed the task of security, and to provide an independent assessment of the progress the FBI has made in reinforcing its security. Specifically, RAND was asked to:

·Assess whether the Webster Commission recommendations, if properly implemented, could lead to a robust FBI security program that adequately protects against another ''monumental failure'' of the Hanssen kind.

·Ask whether additional recommendations are warranted and whether some of the original Commission recommendations may no longer be necessary.

·Consider the critical factors that must be considered during implementation if the resulting security program is to be successful.

·Assess the current FBI security action plan and make recommendations in order that the transformation of FBI security be successful. This assessment and recommendations will include whether the program lifecycle resource requirements and timeline are adequate and feasible.

This report contains responses to the first three tasks, and it conveys some observations about the fourth; without more data, especially on baselines, it was not possible to provide a full assessment of the adequacy of time and resources. The report relies on

interviews and conversations with Bureau and Webster Commission officials, review of available documents and comparisons with other somewhat institutions similar in some respects, inside and outside the intelligence community, such as the Drug Enforcement Administration, the Customs Service or the National Security Agency. The first three tasks are broad, so this assessment responds to them first by recapitulating the key findings of the Webster Commission and looking at the context of security at the FBI. It then works through the components of security in parallel to the organization of the FBI's Security Division (SD) itself - information assurance (IA), personnel security, and physical and technical security. The IA section is more detailed than the others, given both its importance and the special challenges involved in it. In each case, we begin with a basic judgment, then note areas of improvement and make suggestions for refining the program in light of our assessment and the changes in the world since September 11.

WEBSTER COMMISSION RECOMMENDATIONS

As a roadmap, the Webster Commission recommendations sought to establish a workplace culture at the FBI that ''recognizes security lapses as significant, restricts access to particular items of classified information to those who need them to perform their jobs, and makes disloyal employees more quickly visible. If these goals are met, the FBI will strike a sound balance between security and operational efficiency. The Commission surveyed ''best practices'' in the Intelligence Community in framing its recommendation. It focused on ''the structure of the Bureau's security programs and the policies and procedures designed to ensure the integrity of its personnel, information systems, and documents.

The Commission's core finding was that ''although the FBI has begun to take steps to improve security, senior management has not fully embraced the changes necessary to bring Bureau security programs up to

par with the rest of the Intelligence Community. In general, FBI security programs fall short of the Community norm.''

Its principal recommendation was the creation of an ''an independent Office of Security, led by a senior executive reporting to the Director, responsible for developing and implementing all Bureau security programs.'' It recommended consolidating FBI ''security functions, which, in sharp contrast to other agencies, are fragmented, with security responsibilities spread across eight Headquarters divisions and fifty-six field offices."

The Commission also recommended that the new Office [now Division] of Security:

- ''develop programs to address information system security...[for]...the FBI lags far behind other Intelligence Community agencies in developing information security countermeasures. For instance an information-system auditing program would surely have flagged Hanssen's frequent use of FBI computer systems to determine whether he was the subject of a counterintelligence investigation.''

- ''[make] significant changes in the background investigations potential Bureau personnel undergo before receiving initial security clearances and in the periodic reinvestigations on-board personnel undergo for security concerns.''

- ''[make] all personnel ... subject to financial disclosure obligations and ... those with access to certain particularly sensitive information and programs should take counterintelligence scope polygraph examinations during their reinvestigations.''

- ''[develop] career tracks ... for Security Officers to professionalize these positions and make them attractive.''

- "develop effective, mandatory security education and awareness programs for all personnel."

- address deficiencies that mean that "the Bureau does not have a viable program for reporting security incidents to Headquarters. Currently, several components play uncoordinated roles in detecting, investigating and assessing security violations...The Bureau is unable to identify or profile components and personnel who engage in multiple security violations, even when they constitute a pattern."

- "embed security policy development into its management structure to ensure that security programs are recognized and respected and that security is not inappropriately sacrificed to operational objectives...Some of the weakest links in security have resulted from unwritten policies and from of security policies without input from security program managers."

THE CONTEXT OF SECURITY AT THE FBI

Reinforcing security at the FBI amounts to changing its organizational culture. That culture is powerful; it is a source of capacity to act in the public interest. But changing it, like changing any powerful organizational culture, is difficult and slow. The FBI culture prized - and prizes - action; it favored agents on the street over technology, taking, as one special agent put it, a "dirt road alternative to the information highway a decade or more ago." It was and, to a considerable but changing extent still is, a culture of law enforcement. That put a premium on sharing information, not closeting it. The "can do" spirit of the organization makes the gap between headquarters and the field more striking than for virtually any government organization. Most agents want to be on the street catching criminals, not at headquarters pushing paper. The result is that Field

Offices have great autonomy, as is suggested by the Webster Commission's comment that the New York Field Office frequently refused to upload documents to the Automated Case Support (ACS) system.

The FBI's culture is also one in which security, other than physical security, was not a top priority. And while the distinctions have softened over time, still the gap between special agents and ''support'' is yawning. Activities not primarily performed by agents have been given less priority and resources. Technical security was not fully appreciated or supported. Personnel security was seen as an administrative function. The combination of emphasis on law enforcement and the role of agents argued against compartmenting information. Need to know was not really applied in the same sense that it is meant to be applied elsewhere in the government. Even when there existed reasons to do so, the IT systems in place meant that there was not always the means to do so.

Indeed, reinforcing security is a change in culture within a change in culture, for the shift toward counterterrorism is changing the FBI's mission and with it, its culture. In the long run, that change in mission makes the approach of the Webster Commission, which essentially applied an intelligence agency template for security to the FBI, all the more appropriate. Yet, in the short run, the Bureau is being tugged in two directions, characterized by insiders as ''Webster'' and ''9-11.'' While the first argues for being much more careful with and compartmenting information, the latter creates enormous pressure to get on with the job and to share information widely in doing so. Even so, there are very good reasons in law enforcement to restrict access to certain types of information. There needs to be a comprehensive and deliberate approach to information management that enables the work and work processes of the FBI.

In many respects, counterterrorism (CT) bridges the two classic Bureau missions, criminal law enforcement and counterintelligence, reflected in the work of the Criminal Investigative Division (CID) and

the Counterintelligence Division (CD). CID informants, for instance, are themselves criminals who are likely to commit unauthorized crimes. Thus, the premium in handling them is to get their tips, then move them quickly out of the chain of evidence by running an FBI operation. By contrast, while CD assets may commit crimes, many of them are ''white collar spies,'' who may provide valuable intelligence through a considerable period of working for the Bureau. Persons of interest to the Counterterrorism Division (CTD) might be either. They might provide valuable intelligence even as they commit unauthorized crimes, like running guns or laundering money.

Thus, the intelligence agency security template will need to be adapted to an organization that will retain a powerful law enforcement past and continuing mission, and that will be moving toward more emphasis on a counterterrorism mission that crosses intelligence and law enforcement. The new mission is more proactive than the old, more centered on public safety by looking ahead to consequences and planning accordingly.

II. INFORMATION SYSTEMS SECURITY

The steps taken over the last few years to increase information systems security within the FBI represent a clear improvement. As the FBI's information security program is still being built up, further improvement is to be expected. This message is also getting into the field at the leadership level, but needs more attention with individual agents and squads. Currently, five hours are spent on security during initial training - up from two before Hanssen. While opportunities to make security presentations to the whole range of Bureau officials are increasing and while some Field Office security officers will conduct orientation sessions for newly assigned agents, most exposure to security is centered on national security programs and seems tangential to most agents.

The security templates imported from the intelligence community will necessarily have to be adapted to the exigencies of the law enforcement community. That said, the most critical decisions affecting information security are ones that SD can hardly make alone. They require the FBI's top leaders to balance the twin goals of securing information while permitting the kind of information sharing required to meet urgent national goals.

INITIAL CONSIDERATIONS

Information security has three primary facets - the ability to prevent unauthorized disclosure, information assurance (confidence that information has not been tampered with), and unhindered access to information services. All three must be part of a fully integrated information systems security plan. The problems associated with Robert Hanssen were those of unauthorized disclosure.

Minimizing unauthorized disclosure entails:

Explicit formal restrictions (sometimes called ''mandatory access control'' by computer security professionals, that is, being prevented from seeing material one is specifically unauthorized to see);

Implicit informal restrictions (referred to as ''discretionary access control,'' that is, not seeing sensitive material that is not required to carry out official duties); and

Assured implementation of these policies through the correct engineering of information systems.

Hanssen, with a few exceptions, made use only of material that he, technically, had proper access to; there were few or no violations of mandatory access control policies. That he could do so stemmed from the fact that he held a position of great trust. But it was made worse by features of the automatic case support (ACS) and other systems that granted him more access to information than, in retrospect, was wise. Some documents were deliberately made more accessible than they should have been. Others were not as restricted or not as well concealed as they might have been if users had been more aware of ACS's capabilities. At a minimum, therefore, sharply reducing the risks of another Hanssen requires attention to the rules of access. Nevertheless, the need to worry about the technical security of information systems cannot be ignored just because Robert Hanssen did not subvert them. As agents become more computer-savvy (and as so-called " script kiddie" tools proliferate), the odds that some future mole may wreak mischief through computer hacking grow. Still, the policies that govern *who* gets to see *what* bear primary attention.

Since the FBI cannot guarantee that there will not, from time to time, arise people who try to access and distribute unauthorized materials, information security systems should seek to make it difficult, if not impossible, to evade information systems controls and detect as soon as possible attempts to evade such controls.

The achievement of information security requires both people and machines. The best tools in the world are nearly worthless in the hands of those who cannot or will not use them intelligently. Running software that can unearth potentially anomalous activity can only go so far; people must be able to interpret correctly what they see and take the necessary actions based on those interpretations. Management and staff compliance are important determinants of the success of any security program in an organization.

The Webster report makes it clear that the ACS, in general, and ACS's flaws in particular, facilitated Robert Hanssen's ability to pass sensitive information to his patrons. Indeed, in his last period of espionage, he relied ''almost exclusively'' on ACS for his material, downloading several thousand documents. As a result of specific weaknesses of ACS (both in its design and in how it was, in practice, used) he:

-could access roughly 500 documents that ''should have been more restricted than they were, a failure that could have stemmed from ignorance of the restriction capabilities or misunderstanding of how they work''

-could access ''the entire Washington Field Office (WFO) technical program''

-could search ''for documents containing his name spelled several different ways, his home address, names of agents in FBI espionage squads, code names of espionage investigations, Russian/Soviet CI restricted cases, and the word, espionage,'' and

-''found the synopses in the Attribute fields for restricted documents 'very revealing'.''

The Webster report also found that ''frequently a document is sent to a substantive case file, which may be restricted, and to an

administrative file, which often is not classified information from WFO's annual asset reports can be found in unrestricted administrative case files. These reports provide considerable details about foreign intelligence assets, including their identities and activities.'' To put it mildly, there is considerable mistrust of ACS. Several agents believe ''that it is possible to ascertain user passwords by employing ACS system tools,'' and that the system's features have, ''resulted in a number of horror stories about exposure of confidential files on ACS.'' And so, ''personnel charged with investigating espionage allegations generally do not upload case file information into ACS … [and] do not even solicit help with leads on ACS because on one occasion, when a lead was sent to a Field Office, new agents who covered the lead - unaware of the unit's avoidance of ACS [and how ACS file restrictions operate] - uploaded information without restricting it.''

AREAS OF ONGOING IMPROVEMENT

The FBI's information systems (IS) security program can point to many initial indicators of improvement. For instance:

The FBI has begun to pay more attention to IS security (as well as security across the board). Surely, there was plenty of room for improvement. For the most part, there is a firm understanding throughout the FBI that it *could* happen here - again.

The certification and accreditation (C&A) process has come to be both serious and taken seriously. It is fair to note the growing expectation that major projects that do not pass the C&A hurdle will not be ''accepted'' by the FBI. Nevertheless, there remains a problem in ensuring that legacy contracts can be administered in such a way as to permit such requirements to be enforced, and that the ever-present claim of ''operational necessity'' is not used excessively to provide waivers for systems with flawed security.

Computer monitoring has been improved. There is an understanding that retrospective examinations of the Hanssen access logs reveal how anomalous his patterns of access were and that they should have been detected as such. Many people in the FBI had to review their sources, methods, and cases to ascertain whether or not they had been compromised as a result. It is fair to say that the importance of monitoring has been strengthened, and the projected stand-up of an Enterprise Security Operations Center (ESOC) in August 2003 (see below) offers real hope for improvement.

Serious attention is being given to further IS improvements through comprehensive system security engineering. This includes improved intrusion detection systems (with full profiling), role-based access control with reduced sign-on, and token-based public key infrastructure. (PKI).

Housekeeping is improved: people really do get kicked off the roster when they should. For better or worse, people without direct investigative or support needs for ACS are generally not allowed access, even to modules filled with nothing but training data.

The Virtual Case File (VCF), the successor to ACS as the user's standard window into the applications on the investigative mainframe (IM) appears to be getting fixes that would prevent many of the behaviors associated with Hanssen. For instance, under VCF users will no longer be able to look up their own names or the names of celebrities. VCF will also not have the features that resulted in access limitations being stripped from files in several poorly understood circumstances. This improvement, however, raises the question of whether it is better to forbid certain types of behavior, or to permit and then monitor it as potential indicators of more serious abuse. If the latter, do investigators reprimand offenders on the theory that most mildly deviant behavior should be stopped before it becomes a real problem? Alternatively, should they place offenders under intensive but secret scrutiny on the theory that such behavior is symptomatic of more serious

problems? A well-articulated threat model would help in thinking through such issues.

SUGGESTIONS

Although information security entails both correct policies and their correct implementation in software and hardware, the weight of our suggestions falls on thinking through the policies. We believe that the FBI, notably its Security Division, is on the right track in terms of its programs, although only time will tell how much these programs will improve security. However, establishing the policies themselves tends to be a responsibility of upper management because it reflects fundamental issues that define the FBI as an information processing organization.

Improve the Quality of Monitoring Tools

Monitoring networks is universally acknowledged to be an essential component of information security. Indeed, monitoring is often intensified so that systems can be made more open without compromising security as a result. Such monitoring has two functions. One is to determine, often through the analysis of packets, whether illicit activity is going on in the network (for instance, are port scans in progress?). The second is to determine, through the analysis of information flows, whether users authorized to transfer information in the abstract (for instance, download files) are not authorized to do so in the particular (for instance, download files that they have no business reading). Good monitoring of whether people are accessing only files they should must involve those who have an incentive for controlling access - for instance, the squads charged with working a specific case or category of cases. [2]

---

2 It is important to note that good monitoring can often serve as a training tool, as well. Being able to show a squad how an agent successfully used database searches to discern crucial investigative data, or to illustrate

The FBI is planning to set up an ESOC starting in FY 2003; the office head was appointed in August 2002. Tools have been examined to help the monitoring process. One of them, "Silent Runner," can help monitor network patterns against activity profiles that can be developed based on user roles and ancillary personal information. Although these are all encouraging developments, it is clearly too early to evaluate how well the ESOC will be able to monitor and respond to patterns in packet flows or other computer activities.

What needs to be improved is the FBI's ability to monitor activity that accords with the rules of the network but is nevertheless troubling. As noted, many of the records that would have established that Hanssen was a problem were out there to be analyzed but never were (or at least not until the damage had taken place). The ability to monitor file access has become easier with the Case Document Access Report (CDAR), and will continue to evolve as VCF is introduced.

As its primary improvement, CDAR strengthens each agent's ability to monitor who is looking at his or her case files. Indeed, there are new features in CDAR (and, subsequently, planned for VCF) that inform agents whenever anyone who is not specifically authorized to do so examines a document in a file. Exactly how agents should respond to unauthorized accesses when VCF is deployed is a pending policy matter.

In CDAR, agents working the most sensitive cases are currently required to resolve questionable accesses to their case files every 90 days (although, unhelpfully, agent access to access records effectively ends once records are 56 days old). Many accesses are entirely innocent: someone is interested in a topic, pulls up a 25-character synopsis of a document, cannot decide whether the document is relevant, and therefore pulls up the entire document to make sure. Normally, a few seconds' review suffices to indicate that a document does or does not fit the

---

how an agent could improve the effectiveness of their database use, can yield great secondary benefits.

bill.[3] This must happen often. Paying attention to each of these incidents would require agents to spend a great deal of time pursuing explanations for behavior that is not only innocent and commonplace, but is also necessary. Agents are busy people. If they feel annoyed by all this hectoring, they may default to automatically approving every access, which defeats the purpose entirely.

Although CDAR is a useful tool for agents to screen accesses to their case files, it is ill suited for robust analysis of user activities. Its records are available only to the specific case agent; they are inaccessible to local security personnel or to agents' supervisors, much less anyone higher up the chain. CDAR only indicates case access activities, and does not really offer a query capability. To do so requires a different, comprehensive audit analysis tool. Even though patterns of unauthorized access may only be apparent when multiple cases are examined, it is impossible using CDAR to make queries that might, for example, indicate which agent has pulled the most documents from other agents' cases. Nor is it possible to monitor a pattern of activity that is more than eight weeks old without going back and pulling tapes (and present policy is that only the Office of Professional Responsibility and SD investigators can request this). By contrast, good monitoring practice should make it easy to follows hints and hunches by creating queries on the spot.

We therefore make three strong suggestions:

Develop, under Security Division auspices, a more robust set of tools to keep tabs on any file access activity that may be construed as anomalous (without necessarily having to start with a name request). For

---

3 Ironically, the move from IBM 3270 terminal emulation to web-based browsing will blur the distinction between a quick pass and a long examination of a document. One can tell how many seconds a document has been viewed via 3270 emulation. In a web-based environment one can only tell how long it was between when two documents were called up, but the first one does not necessarily disappear when the second is pulled. It would not be hard for a mole to game such a system.

instance, ''who has looked at the most counterterrorism files last month?'' ESOC will need such capabilities, and there should be serious thinking about how to get them in place before it begins operation.

In an era when 80 to 120-gigabyte hard drives are standard equipment on home computers, there is no good reason not to put the FBI's entire access history (for instance, since 1995) on immediately accessible storage media. By doing so, those responsible for 90-day reports will have all such data at their disposal. Our rough assessment is that the volume of the audit data currently generated by queries to ACS and the Universal Index system was no more than 20 gigabytes per year.

Review the requirement to have agents resolve every anomalous file access in order to focus on those accesses that are of more potential concern. Multiple accesses within a case or across similar cases may, for instance, be indicative of improper access; so might accesses at odd hours. For this purpose, CDAR might be enhanced to automatically dismiss document accesses lasting only a few seconds, unless there was a pattern of repeated accesses or unless other specific criteria were triggered (for instance, particularly sensitive case classifications). The effectiveness of these types of ''smart'' CDAR reports would depend on the operating environment, and many factors would need to be taken into account. Still, these smart reports might provide an interim, agent-friendly approach to resolving case accesses. A parallel requirement to resolve a random sample of CDAR anomalies would make it less feasible to ''game'' the smart system.

Better Separate Counterintelligence As Well As Asset and Informant Data

The problems with how ACS was used, so blatantly apparent in the Hanssen case, indicate that users need to be better educated about FBI's information systems. Some users were unaware that they could restrict access to documents; other users revealed information from restricted

investigative files in unrestricted administrative files. Several capabilities resident in ACS (e.g., multi-factor search) are unknown to many users (c.f., Agent Rowley's well-publicized complaint that ACS does not allow multi-factor criteria). But security should not *depend* on such education being 100 percent effective.

In particular, there are good grounds for believing that counterintelligence data should be taken off ACS and put onto its own system, at least to the point where someone could not start with basic access to ACS and end up with CI documents. Separation of CI data onto a separate virtual private network (VPN), accessible only by CI agents and support staff, would be one approach to solving this problem. Doing so would mean that mistakes in document management would not create leaks outside the counterintelligence community.

This would put more emphasis in managing need-to-know closer to where access can make the biggest difference. It would also present one more barrier to someone using computer hacking tools and skills to penetrate sensitive files. Finally, a separate system for counterintelligence would make it that much easier to monitor the circulation of Foreign Intelligence and Surveillance Act (FISA) data. Granted, Hanssen *was* a member of the CI community; but the next mole may not necessarily be.

Segregating counterintelligence data from the mainframe has some downsides. First, it would impede the access to such data from outside the CI community. This is perhaps a particular concern to the CT community, for just as the counterterrrorism mission bridges traditional Bureau missions, so, too, does it involve FISA data. Only time will tell how frequent the need for crosswalking such information will be, and those agents who do need repeated access to CI documents can be granted access privileges to the CI system for the interim. Second, if the separation were done in hardware rather than software, it would be mean one more system to manage, especially if encrypted tunneling is used (see below), but servers themselves are cheap. Third, although stripping

CI data off the mainframe would reduce the consequences of its compromise, there is a residual risk that people will therefore take the mainframe's security that much less seriously.

Specific data on informants, held on CIMS, the Criminal Informant Management System, is some of the most sensitive information that the FBI has. This CIMS information is, appropriately, isolated from the rest of ACS. Furthermore, the pains that some agents have taken to hide identifying information about informants (for instance, doing National Criminal Information Center queries on them without associating such data with specific cases) adds a further layer of protection. Nevertheless, we have lingering concerns about the treatment of informant data. This data currently resides on the investigative mainframe, along with other applications, and the existing software access controls do not offer a high degree of protection. Having CIMS data on a separate network or sub-network, perhaps virtual, would be preferable but would carry some of the same downsides as doing so for CI data.

Access controls would also be reinforced by better protection of Counterintelligence and Criminal Informant information as it travels over FBI Field Office LANs, over which these data are currently carried in the clear. In theory it is not hard for a user to sniff all the traffic on an office LAN and capture the packets of interest. As a security precaution, therefore, these particularly sensitive data moving from server to client should be handled via encrypted tunneling.

Improve Feedback on and Responses to Security Flaws in Legacy Systems

There are also concerns relating to certification and accreditation (C&A) of existing, fielded computer systems. In these cases, the Security Division often has much less leverage. For example, if critical flaws were to be encountered in the certification or accreditation processes of a major system such as ACS, it would be

impractical for Security Division to insist that the system be taken off line until the deficiencies were addressed. There is simply too much reliance on ACS throughout the Bureau to allow that to occur. In the case of systems that are not as critical to ongoing operations, Security Division should be permitted to exercise its authority to withhold accreditation from systems with particularly egregious security vulnerabilities.

Yet, complex software is inevitably fielded with potential security flaws. This is particularly so for legacy FBI software for which C&A has been missing or cursory. Users should be encouraged to - not discouraged from - experimenting with all of the features offered by the software in an effort to find security flaws (even if only a small percentage of agents are of a mind to do so). Such flaws, if found, should be immediately addressed (and feedback to interested users should follow successful patching). It may also be useful to run periodic tests to match file accesses with privileges of those who accessed them, in order to identify cases of access that should not have happened had the system been working correctly (or according to the strictest applicable access rules).

Continue Vigilance over New Systems Development

Ultimately, the leverage of the Security Division over the security of information systems throughout the FBI will be demonstrated through the continuing role of Security Division in the C&A of new computer systems. The C&A process represents the opportunity of the Security Division to exercise control over computer systems in their developmental stages, with the specific goal that any computer system must meet fundamental security requirements.

It is, of course, imperative that the C&A process be well defined, and that the security policy that the system is expected to enforce is well understood by the system developer, the user community, and the

teams conducting the C&A. Once all participants understand the security policy constraints, the processes of development, C&A, and deployment will be greatly simplified. Unfortunately, the FBI currently lacks a clear delineation of certain security policies (especially those relating to law enforcement sensitive information). This only adds to the difficulties of trying to establish reasonable requirements and metrics for security, and hence leads to specific challenges in information system development, certification, and accreditation.

The most immediate and pressing such case is the Trilogy system, which represents hundreds of millions of dollars of investment in desktop, server, network, and software infrastructure. Because VCF (the primary user application (UA) component of Trilogy) will directly replace the investigative mainframe functions currently imbedded in ACS, the development of a credible and sensible security policy for this system is of vital importance. Likewise, the assurance that the system correctly implements this security policy to a high degree of confidence is fundamental to the basic principles for which the investigative mainframe computer systems were originally intended, and which the Trilogy program hopes to bring to fruition.

Unfortunately, the need to field Trilogy as an operational system on a very tight timeline risks a "lose-lose" scenario. Current plans to do performance, functionality, and security testing in parallel raise a host of issues. Important security functions may be omitted from the initial Trilogy release, with a promise to retrofit security mechanisms onto the system. Should there be significant security-related difficulties encountered with Trilogy in the future, it will almost certainly be impossible for Security Division to exercise its authority to "pull the plug" on the system (or any of its components) pending remedial action. If Trilogy becomes the backbone of the FBI information technology architecture, any flaws will need to be addressed through work-arounds as they become available. If, after all this, there are perceived security shortfalls in Trilogy, the system could fail to win the trust of agents in the field just as ACS is not trusted today.

Trilogy's tight timetable exacerbates these problems of credibility. Although the first phase is scheduled for December 2003 delivery, first-order requirements gathering was completed only in September 2002. That left only fifteen months to compile and validate an integrated set of requirements, design the system, code it, test it for functionality, tune it for performance, and then and only then begin, conduct, and complete a full C&A process. The lack of a fallback risks that the new systems will be accepted even if after-the-fact security faults are discovered simply because there is no longer any alternative.

Trilogy does not have a requirement for multi-level security. It is system-high SECRET, which means that all information on it is treated as SECRET regardless of how that information is labeled. (The FBI chief information officer is exploring the idea of running the FBINet at a higher level of classification, or on a multi-level basis.) The C&A process must ensure that users can trust that security classification markings they enter on specific documents will be retained by the system. Otherwise, future users could compromise security without realizing they were doing so.[4]

Finally, while Trilogy and ACS have been the focus of this section, the need for early and continuous involvement by Security Division in the development and C&A process of all new FBI systems cannot be overstated. There are reasons to believe that many features that give rise to concerns over Trilogy - ambitious goals, fast timetable, and subsequent pressure to meet milestones - could recur in the Integrated Data Warehousing program. The Security Division is correct in its

---

4 Note that Trilogy will also be fielded in FBI-hosted Joint Task Forces where there are a mix of FBI and non-FBI personnel. Although anyone with access to FBI systems is appropriately cleared and vetted, many task force personnel have not had the benefit of FBI training in information security and proper document classification. They may thus be more likely to take document markings presented by VCF at face value, while FBI employees might recognize that the document is more sensitive than the markings indicated.

belief that security must be continually addressed as this program moves forward.

Restore Faith in the FBI's Investigative Mainframe

The New York Field Office appears to be unique in this respect, but the fact that some of its squads have "do not upload [to ACS]" rubber stamps that are used frequently by counterintelligence agents indicates that the skepticism about the security of ACS noted in the Webster report persists. There is, however, less reluctance by squads dedicated to counterterrorist and criminal investigations to use ACS to support their work.

The road to convincing agents that the investigative mainframe computer and its applications, like ACS, are trustworthy will be a difficult one with no guarantees, but there are some steps that could help:

First, encourage people to give Trilogy a hard road test, if they so choose. Encourage them to find security faults with it and recognize their contributions (rather than take away access privileges as happened to one NYFO agent who reported what he believed were flaws in investigative mainframe applications). Even though the discovery of faults may reduce confidence in the system itself, the demonstrated fact that the FBI takes such faults seriously and wants to see them brought to light should improve their confidence in the process by which the system is managed.

Second, encourage a rigorous program to shake the bugs out of VCF—called beta testing program—*before* VCF is fielded.

Third, train people on VCF when it is fielded. In particular, make sure they understand how their actions affect the accessibility of documents in case files.

Do Systematic Analysis of Need-to-Know

Although the Robert Hanssen matter focused attention on need-to-know, aspects of need-to-know control have long been part of ACS. Documents on ACS have, almost from the system's inception, been characterized as, alternatively: (1) for everyone, (2) limited to those in the originating office (''O''), or (3) limited to named persons (''P''). Earlier discussions considered a designation that would limit access to persons within a squad (for instance, a sub-office) but that never came to pass.

Since the summer of 2001, the mandated default settings on documents in specific cases have swung back and forth. In this case, the concept of ''default'' goes well beyond ''if the user does nothing, the following will be true.'' It really means that documents will be restricted as per this guidance absent the permission of the assistant director with oversight over such cases (for example, the assistant director for counterterrorism has oversight over all ''199'' cases). In practice, therefore, default is governing in all but exceptional cases.

Fluctuations in the access restrictions on counterterrorism cases have been striking. Prior to September 11, counterterrorism cases defaulted to office (''O'') restriction. Data from the Y2K bomber (Ahmed Ressam) was kept particularly close hold. Many counterterrorism agents chafed at such restrictions. In mid-October, during the PENTTBOMB investigation, the policy was completely reversed. Counterterrorism cases defaulted to unrestricted access and even FISA data was being more broadly shared. As the PENTTBOMB investigation wound down (and the number of FBI agents assigned to counterterrorism declined), new guidance was drafted that, by default, limited access to such files to

named individuals. It is by no means certain that this is the last word on the topic.

Admittedly, the problem of balancing security and need-to-know without undue harm to either is a complex one. But this is precisely why *it needs nothing less than the best and most considered analysis.* Although there are plans to develop an analytic capability within the Security Division, the decisions on need to know are properly those of corporate management and would involve most of the various assistant directors.

Implementing need to know so that such controls are easily accessible to system users would be a technical improvement that would facilitate the transition between security policies and security practice. Briefly put, it should be no harder to put together an access list for ACS/VCF than it is to assemble a "to" list for a modern E-mail application. A capability to build lists through point-and-click access to user lists or through successive aggregation may help.

Another innovation worth consideration would be to create broad membership groups to which documents could be restricted. One such group might be composed of every agent in any counterterrorism squad (roughly 20 to 25 percent the agency's total manpower). A counterterrorism case that restricted its documents to that group would be put off-limits to most of the FBI's agents, but those who needed to "connect-the-dots" would be able to see the material that would best help them.

Finally, the issue of how much to show non-FBI participants in FBI-led joint task forces needs systematic consideration. Field Offices are confused by current rules, with some task forces getting access to nearly everything and others given access to nearly nothing. When task force members are allowed to see only 3 out of 47 cases returned by a query (as was demonstrated in the case of one NYFO task force member), the rules under which such access is governed may not be easy to infer.

Communicate Security Requirements Clearly

As a general proposition there needs to be a set of clear expectations about the future information security environment so that everyone is planning with a common set of expectations. Understandably, many of the issues are under active debate, but the earlier a clear resolution is achieved, the better. For example:

Will Trilogy operate in lock-down mode? Some people believe that when Trilogy is implemented it will be impossible for employees to store any data on removable media or on their local hard drive (except for local caches); even printing will be a more complex maneuver. Others believe that this condition will prevail in large offices but not in small ones. Still others foresee a clampdown on removable media and laptops but not anything similar to a lockdown.

Will there be sub-document classification? The customary practice within the defense and intelligence communities is to indicate the classification of every paragraph within a document. Will the FBI change its practice and adopt this convention? Some say yes; others say no. Complicating the issue is the fact that there is little guidance about how to have systems enforce specifically marked paragraphs or how to display them correctly in an online (for instance, Web) document. Further, if the administrative mainframe is expected to maintain document security markings, then a system that manages paragraph-marked documents is much more complex to implement than one that manages classification markings only at the document level.

Who will be responsible for certification, who for accreditation? The FBI's former chief information officer would have had the Bureau's Information Resources Division (IRD) take responsibility for certification while SD took responsibility for accreditation. The argument has been made in SD that the reverse should prevail: SD certifies and representatives of users accredit. Why? The decision to accredit a system should reflect not only its security but also is

appropriateness for the job at hand. In August 2002, recommendations were made to DOJ (Security, CIO, and IG) to realign certification responsibilities to security and accreditation responsibilities to FBI's CIO. At the time of our interviews (August 2002) there was little evidence that many people recognize that this change is coming. This situation may have clarified itself in the subsequent months.

III. PERSONNEL SECURITY

Here, too, much has been accomplished. The Bureau has moved to tighten and professionalize the Security Division and to upgrade the investigation and reinvestigation process, and it is expanding the use of the polygraph, which it conceives primarily as an investigative tool despite its increasing importance in screening. It is moving to implement financial disclosure, though it plans for a very gradual implementation. The Security Division is also exploring better methods (for instance, web-based) for collecting and processing security and financial information. This will help speed internal processing and work to eliminate keyboard entry errors during transcription. It is moving toward developing a professional security cadre, mostly by hiring from the outside but also by making available opportunities for existing officials who might be interested, both agents and non-agents. There are questions about the Bureau's approach - and we make some suggestions on that score - but in this area the main issues concern the resources, people and time necessary to change procedures and to make them part of the FBI's organizational culture.

INITIAL CONSIDERATIONS

Among the truisms of security is that systems and technology matter, but people are decisive. No matter how good any organization's security, it may still hire an occasional bad apple, and, more to the point, apples occasionally will turn bad. The challenge, therefore, is, as the Bureau puts it, to reduce the gap between "defection and detection" - to notice indicators of particular trouble as soon as possible. In retrospect, there were indicators aplenty of trouble with Robert Hanssen. Yet those tended to be dismissed, entirely understandably in human terms, as bad spots in his life or just more evidence that he was an odd bird. That tendency was reinforced by a

powerful aspect of the Bureau's culture - the sense that agents, once through the arduous winnowing process of gaining admission, are a band of brothers, now including many sisters. ''Who are you to question my trustworthiness?'' is the attitude that results.

The approach to personnel security was, and is, ''tiered'' security. The inner tier is counterintelligence, counterterrorism (CT) and security, on the argument if those areas are penetrated, the national security is at risk and lives can be lost.[5] By contrast, if organized crime turns an FBI agent - such as John Connolly in Boston - it is embarrassing but not deadly. Now, though, perhaps a quarter of the organization is working on CT, and so in the short run sheer numbers are a problem. In the immediate aftermath of September 11, 7,000 FBI officials were working on CT. Given that agents move from one area to another - especially, now, from CID to CT - the inner tier is and will remain large.

The second aspect of the approach is a focus on reinvestigations. As the Hanssen case demonstrated, those had been *pro forma*. Yet it is less likely that an FBI official will be ''born bad'' than that he or she will be turned bad by midlife crises of money or relationship or self-esteem, especially the first. As one FBI official put it, Americans become spies for three reasons - money, money and money.[6] Thus, along with an emphasis on reinvestigations, financial disclosure and other ways to follow people's finances are critical.

The third aspect, here as in the rest of the security program, is risk management. Many of our suggestions go in the direction of broadening the application of that principle. If the governing principle were risk avoidance, the Bureau simply would not hire the contract translators it is now bringing on board in large numbers. Risk

---

5 This needs to be thought through in a clear deliberate process since one could also make the argument that CT cases also require a more open information environment as the Bureau seeks public safety over pure reactive law enforcement.

6 The recent case of the spy for Cuba, Ana Montes, is an exception, one suggesting that the line about money should not be taken too literally.

management implies hiring them but maintaining a special watchfulness for indicators of concern.

AREAS OF ONGOING IMPROVEMENT

Professionalizing Security

Establishing a distinct Security Division was a major recommendation of the Webster Commission, and it has been accomplished. From our interviews, the senior managers of SD mostly got high marks for effectiveness and for understanding the culture in which they operate - the second observation was notable because most of them are not FBI careerists. The Hanssen debacle was searing enough to drive home the realization that security had to be taken more seriously, and the program managers have taken advantage of that opportunity.

By the same token, the plan to professionalize security by beginning to create a career track also makes sense. At present, security usually is a collateral duty, not a primary one; that is especially the case at headquarters components. As such, it has not been an attractive assignment. Agents assigned as security officers sometimes have delegated most of the responsibility to their non-agent alternates. Security officers in Field Offices work for those offices, not for SD. Security officers have had neither time, nor knowledge nor materials to be very proactive, to reach out to colleagues and spread understanding of security and its importance.

Security officers in the Bureau's operating units are crucial links in the security chain. For reinvestigations, they receive the list of those up for reinvestigation in any particular month. The SD passes to them the form - the Bureau uses its own form, FD-814, not the SF-86 form used by most of the rest of the government. With the form in hand (getting it back has been the hardest part), the officer conducts the PSI, personnel security interview, which focuses on the usual concerns over money, partners, foreign contacts, and the like. The package will

then go to the SD, returning to the unit security officer if issues arise about which SD would like more answers.

Now, security officers get training only on the job; there is an annual conference for security officers, but not all attend, especially given that for many the assignment has been one from which they were trying to escape. Those that do attend may only attend one year before being replaced with another person. In addition, each may have a completely different set of duties. The current plan is to bring in professional security officers - from the outside if need be but also giving opportunities to insiders, including agents - give them a basic course, then have them come to headquarters on temporary duty both to help out and be mentored. The big three offices - Washington, New York and Los Angeles - would have GS-15 security officers, providing security officers from other cities with head-room for advancement. They would also be responsible for the full range of security at any location and for advising the special agent in charge (SAC) on security matters in the normal execution of duties at that location.

This assessment did not take us to more than a few of the FBI's 56 Field Offices or to many of the over-700 FBI facilities around the world. However, in those we did visit we heard the perception that security policies are not being consistently applied. More work needs to be done to see how well the new approach to security programs and policy by the Security Division gains acceptance. At the sites we visited, as well as in the headquarters, where security personnel were becoming recognized for their contribution to the FBI's overall mission, they were more successful. In those cases, security tasks tended to be concentrated in a security organization reporting to the executive head of the office. In contrast, where the security function was still thought of as an administrative function, it tended to be fractured, spread among several different divisions and contractor personnel. Personnel security might report to the executive head, but with physical security, computer security, and sometimes document control reporting to

various internal FO divisional heads, thus leaving no senior officer in a position to advise the SAC on security matters.

It has been suggested that security officers in Field Offices report to Security Division at Headquarters, as opposed to the Field Office SAC. While this would help provide consistency in implementing Bureau security policies, it would also take one tool away from the SACs in managing their operations. Plainly, the SACs need a professional security officer to manage security programs within the office. The challenge is to build processes and career paths that retain the SAC's authority while building close ties to security organizations at FBI Headquarters. The priorities for Headquarters are institution-building that provides career support, education and training, security reachback support, research and development programs, and Bureau-wide policy.

Upgrading Reinvestigations

Reinvestigations, as the Hanssen case testifies, were not high priority. Often they simply languished, sometimes for years, as officers moved from post to post, one step ahead of their reinvestigation paperwork. Now, with additional manpower, the process is more systematic, and SD has created an Analytic Integration Unit (AIU), composed mainly of retired agents, to give a special look at old cases or new ones that pose problems. The analytic unit has 17 people, and is scheduled to grow to 31.

Overall, the SD opens about 7,000 reinvestigations cases a year. Two years ago, 1500 reinvestigations were overdue from the Field Offices; now the number has been cut to 150, and in general relations with FOs and with the SACs are much better. Security is no longer just "blown off." In keeping with risk management, SD might make more use of variable reinvestigation cycles. Now, given concerns about contract translators (260s), they are to be reinvestigated as often as every year. For officers about whom no whiff of concern arises - from

supervisors, co-workers or automatic flags - the cycle might be stretched to seven years, for instance.

One small change would be helpful. The SD now has a target of six months to complete a reinvestigation. That number is arbitrary, apparently an old estimate of how long the process should take. Other agencies' target is one year. A year would make sense for the Bureau as well. The important thing is to keep the process moving. If it is moving, then providing time for a closer look is all to the good. If reducing the numbers backlog becomes the main objective, the result is likely to be more cursory assessments.

Making More Use of the Polygraph

The history of the polygraph for personnel issues at the Bureau is a decade old, beginning with its use when ''issues'' arose in particular instances. It began being applied to new applicants in 1994, and now the Personnel Security Polygraph (PSP) - a CI, not a life style polygraph - is used for reinvestigations of personnel assigned to counterintelligence, counterterrorism and security programs. Not all personnel with SCI (sensitive compartmentalized information) access are polygraphed; it is applied to some, legal attachés, for instance, regarded as in especially sensitive positions. Use of the polygraph is becoming more institutionalized, although it still clashes with the culture of ''we've worked hard to get here, we're good, so don't second guess our loyalty.''

The Bureau distinguishes its philosophy of polygraphing from other agencies, particularly intelligence agencies. It does not regard the polygraph as a reliable screening tool; rather it is an investigative tool best used in the hands of a skilled investigator.[7] The more

[7] This is the view of a forthcoming National Research Council study, The Polygraph and Lie Detection, see http://www.nap.edu/catalog/10420.html: The polygraph is more likely to be valuable if the question being asked is very

specific the question being investigated, the more reliable it is. That said, as the polygraph program expands, it is becoming more of a screening program. The Bureau regards the screening as particularly efficient for new applicants, where it can, for instance, identify problems of truthfulness in applications, thus saving money and time. Over time, the Bureau will wind up polygraphing essentially everyone. It is appropriate, though, while using the polygraph for screening purposes, to regard it as only one instrument among several. Doing so is all the more appropriate given the FBI culture.

SUGGESTIONS

Reevaluate How Informants and Assets Are Managed

This remains a problem without an obvious solution. Current arrangements do not seem appropriate on either operational or security grounds; little has changed to inspire confidence that another Hanssen could not compromise the names of those who have been recruited by the Bureau. The area is one in which the crossing of intelligence and law enforcement in CT imposes special complications.

Traditionally, the Bureau had ''informants'' on the law enforcement side and ''assets'' on the counterintelligence side - now it has about 10,000 total, perhaps two-thirds informants - and the divisions with operating responsibility handled their respective informants or assets. Then, the two units were joined in an Asset and Informant Unit (AIU) when the Intelligence Division was created. When that division ended, the AIU stayed together but was moved to CID. Yet the merger has been mostly on paper; AIU is, in effect, two system stitched together. Given CID's law enforcement focus, the ''asset'' side of the unit takes second

---

specific and investigative - did you pass that document improperly yesterday? - rather than a broad screening question about, for instance, drug use over a lifetime.

place. For instance, it used to have a staff of ten but is now down to four.

Operationally, an argument can be made either for keeping the AIU together or for splitting it. If it is kept together, it should be moved to somewhere that is more evenly interested between informants and assets, the Office of Intelligence or the Office of the General Counsel, or perhaps, SD. The argument for keeping the office together is to facilitate moves across categories, especially in CT. An informant on domestic terrorism might be used by CD or CTD if, for instance, Syria approached a white supremacist group. Eventually, that informant might be better handled as an asset.

The argument for splitting the AIU is to give the operating units more direct control over their informants or assets. Splitting would mean "three sets of books" because CTD would have its own informants/assets, with its own procedures for how to handle them. At present, since most agents who move to CTD come from the CID side of the house, they are more familiar with the rules and procedures for recruiting informants, and so are likely to move possible recruits into that category, not the asset category.

On the security side, the asset database, now classified SECRET, probably should be TOP SECRET, more like asset information elsewhere in the government. The informant database is Law Enforcement Sensitive. The Intelligence Community has developed the Human Intelligence (HUMINT) Control System (HCS), now in use by the CIA, which operates as a SCI channel. At present, though, HCS is unfamiliar even to those in AIU. Asset and informant data are on separate databases, and asset data is not uploaded into ACS. A one-page description of each asset is not supposed to be taken from the secure file room, and on the informant side, too, names and other details are supposed to be restricted to the agent, his or her superior and a small number of people at headquarters.

Especially given the Bureau's culture, though, classification is probably less important than people factors - how the rules are observed. When Hanssen was assigned to the State Department, his access to sensitive FBI information should have been curtailed, but that did not happen. On the basis of anecdotes, he was not unique; in other cases, senior officers raised a fuss when they were denied access to information they had no need to know, and as a result did receive access.

Implement Financial Disclosure

If officers are turned bad primarily with money, then watching the money trail is imperative. Now, finances arise mostly in connection with reinvestigations. The Bureau plans to begin financial disclosure after the first of the year, on a small scale, with analysis of the disclosures done by experts not yet hired. Disclosures are particularly helpful in gaining information about the finances of spouses or partners; absent that information, changes in an official's spending habits can be dismissed as a result of a spouse's inheritance - as was the case with CIA traitor, Aldrich Ames.

This seems an area where the pace could be pushed, signifying the change in priority to security. Numbers are daunting, given the total Bureau population of 28,000. Yet, while filling out disclosure forms is a nuisance, it is a minor one; many American homeowners have done something similar more than once this year in refinancing their mortgages. And spot checks would be a deterrent, or a very hasty review by experts could spot obvious anomalies.

Over the longer-run, in this area as others, the goal would be a series of automated flags. Disclosure forms online could be searched automatically against preset criteria, looking for income or expenditures numbers that seemed out of scale. Now, expenditures can be

checked against income only in the five-year reinvestigations, and then only with difficulty.

Merge Suitability with Security for New Hires

In making new hires, the FBI divides suitability and security. The Bureau Applicant Employment Unit (BAEU), part of Administrative Services Division (ASD), oversees the investigations and makes determinations of suitability. The SD then, in effect, reviews the file to make its security determination. Especially given the burgeoning numbers of new entrants - 900-plus new agents in FY02, for instance - there is a strong argument for merging the two processes, that is, for having a single process apply two somewhat different sets of criteria.

The Field Offices take the lead in recruiting and in handling the paperwork. The procedure is somewhat different for various categories of new entrants - agents, general clerical support people, more specialized support people and contractors. The would-be agents go through a testing procedure, and the applicant testing units conduct many different tests for different support specialties - linguists, police and the like. Not every particular specialty can be captured with a test, and so in some cases, budget analysts for instance, the staffing units will assess the qualifications of particular applicants, then certify to BAEU whether a given applicant meets the qualifications.

Most of the time, the Field Offices in whose territory applicants reside set the leads for BICS (Background Investigation Contract Service), which arranges for the background investigation. The materials then come to BAEU as a "hiring brief," to be reviewed and a judgment about suitability made. SD then makes it determination of clearance based on the same package, though it can return to BICS or the Field Offices with additional questions. In the case of contractors,

while linguists get DoJ clearances, many other contractors are cleared through Defense channels, the Defense Investigative Security Clearance Office (DISCO).

In principle, that merging of suitability and security could be done in either ASD or SD. In either case, training would be required to permit a single specialist to apply two sets of criteria. In practice, though, security is probably the ''long pole in the tent'' in the sense that while some applicants might be judged suitable but still not be clearable, the opposite would be extremely rare. (The rare instances might be drug use, where the very restrictive FBI policy could render an applicant unsuitable even though he or she could be cleared under, for instance, the standards of intelligence agencies.) Merging the suitability and security procedures in SD would make all the more sense if BICS were moved there as well. There would be a single focal-point for setting leads and dealing with BICS. Some training and some moving of people would be necessary to apply the two (overlapping) sets of criteria for suitability and clearance, but simplifying the process would be worthwhile. Already, the BAEU is considering taking on board some BICS staffers, in an effort to better connect to the investigations process.

Oversee and Restructure BICS

BICS (Background Investigation Contract Service) is the Bureau's investigative unit, which manages about 1400 contract security investigators (SIs), about four-fifths of whom are former FBI agents. Attached to the ASD, it conducts investigations for several Bureau elements, including SD; in total, it does about 25,000 investigations a year. Part of its problem simply is that is has grown very fast; it covers too large a span to be managed well. In the normal course of a reinvestigation, SD will do the credit check, then set the terms for BICS's investigation. The results then return to SD, and if the SD specialists spot something that suggests another interview, they can ask

for it. Ultimately, the complete case is written up by a personnel security specialist in the reinvestigations unit, or by the analytic unit, along with a recommendation or adjudication.

SD has asked to take over BICS but not pressed the case, given other priorities. It would be natural, though, for SD to manage BICS and to seek both more efficiency and higher quality. In the process, BICS could be restructured to outsource most, perhaps all, the investigations. Outsourcing would make hiring and firing of investigators purely commercial decisions, would give SD tighter oversight of the SIs, and it would lead to better technology. Now, for instance, SD officers regard the quality of BICS investigations as very varied. SIs are uneven in how diligently they follow leads, and in how rapid they are in doing so. BICS does quality control manually, but competing companies automate it. Outsourcing is objected to on the grounds that "strangers" would be doing the investigations, but in fact many of the 1400 current BICS contractors also work for other companies now.

Provide More Opportunities for Security Education and Training

Currently, only five hours are devoted to security training during initial agent training. While it is difficult to determine precisely whether this is enough, some increased emphasis on security issues almost certainly is warranted. If security is to become part of the culture and work process, then it should be at the core of FBI course work as well. Opportunities to learn security technique within the current course flow could be better exploited - for example, the place to reinforce technical security techniques may be during training that uses radios or ACS need-to-know during computer case study/document processing. In addition, due to the rapid changes in both technology and threats, there is a need for in-service education and training for intermediate and senior level personnel. While this may be more

important for technically-trained agents (TTAs), all agents should receive periodic updates.

SD already has an internal Web site, and it could be developed, first, to provide easy access to documents and answers to frequently asked questions (such as "What do I do if I am about to marry a non-American?). With sufficient resources, the site might also be a place where Bureau officers could go for answers to specific questions, on either an anonymous or confidential basis. Other agencies, such as the National Security Agency, have experimented with security booths, ones that provide information about security and perhaps other issues, as a way of both raising the salience of security and signaling that it can be an enabler, not an obstacle.

IV. PHYSICAL, TECHNICAL, AND DOCUMENT SECURITY

As the new emphasis on security takes root at the Bureau, much of the daily contact that FBI personnel have with security revolves around their entry into FBI workspaces. Thus, this aspect of security, like information security and more so than personnel security, directly affects the workplaces and work processes of the FBI. Since almost everyone has access to secure documents, FBI officials make daily decisions involving the "need-to-know." They also use cell telephones, fax machines and other electronic personal digital assistants (PDAs). In addition, outside personnel can enter secure FBI workspaces, where they often expect access to FBI computer systems. The tension that runs through all this assessment - how to clamp down to guard against future Hanssens, on the one hand, but how to cooperate more and provide greater access in combating terrorism, on the other - arises is spades in the three dimensions considered in this section.

At best, security should be considered an enabler embedded within work processes, thus requiring a balance between the need to share information among diverse work groups and the risk of inadvertent or deliberate compromise. Physical and technical security create demands on facility design, work process organization, personnel vetting, certification of venders and contract workers, and the personal professionalism that all FBI employees bring to their work with the Bureau. Generally, security policy is most successful when security practices are endemic to work practices. As is true for safety as well, security practices can fail if they are merely tacked on.

Decisions about two of the three dimensions, physical and document security, are centered in the Security Division, at least at FBI headquarters. (Security in the Field Offices can still be split among several divisions.) Technical security, however, remains spread across two or more divisions. In addition to SD, the Investigative

Technologies Division (ITD) provides technical support, primarily to overseas assets and national security programs. As the culture changes and the Bureau adopts more technologically advanced means for doing its work, the need to develop a unified policy for technical security issues will grow.

INITIAL CONSIDERATIONS

The Webster Commission made only a few recommendations directly affecting the physical security of FBI facilities. It did, though, make clear that the insider methods Hanssen used to find sensitive information and move it out of FBI facilities hinged on his ability to gain access to areas in which he should not have been able to move unescorted.[8] The first line of defense against technical attack is the ability to fully control access and to limit it to cleared personnel. Physical security also relates to the degree of protection provided employees of the Bureau, detailed Task Force personnel, and contractors working in and around Bureau facilities. Needless to say, in the aftermath of the September 11 attacks, increased physical security for U.S. facilities abroad as well as at home has become the watchword of every government agency.

---

[8] The Webster Commission notes that Hanssen (as well as Ames) was able to walk into meetings uninvited, collect Top Secret and special handling documents in areas that he was not working, and take other actions made possible by his ability to gain physical access without a need to know. Given tighter controls on access, as well as on egress (for instance, inspection of what employees take out of the building), FBI security personnel could have interceded to prohibit Hanssen's following through on his collection of material for the former Soviet Union. Best practices in physical security call for a layered approach. The first layer extends just beyond the physical borders of a facility; the next layer, to the borders and entranceways; then, internally, though the use of card readers, surveillance devices, or other technology (locks, safes, and alarms). All layers attempt to protect information from people who do not possess either appropriate clearances or a need to know. Physical security practices not only guard against harm to individuals but also help protect institutions and their work processes.

Maintaining the Secret-level FBINet as the central FBI tool places demands on how FBI workspace is maintained and access controlled. These demands affect all Bureau activities involving the use of information technology. A Joint Task Force, an FBI legal attaché (LEGAT) at a U.S. embassy abroad, a small off-site office in the Midwest - all need to be protected to the same high standard if they have access to FBINet. Those demands are only increased because many of the physical security standards the Bureau confronts come from the agencies and other government organizations that own and control valuable information. In recent years, the utility of that information has increased, not only for traditional criminal cases but also as the Bureau mission has shifted toward counterterrorism.

Many of the FBI managers and security personnel we talked with stressed that the first line of defense was to maintain good access control.[9] Physical access to FBI facilities is a responsibility of each cleared individual. Today, with the Bureau being the designated lead for several Joint Task Forces working on a variety of issues, its labor force in the field approaches a one-to-one ratio of FBI personnel to outside personnel. This places unprecedented demands on what was once a closed culture. If cooperation is one of the keys to successful law enforcement, the Task Force environment takes it one step further in seeking collaboration within a common work process.[10] With access to FBI systems and space come special considerations for background checks and proper vetting, which is then augmented by security procedures and

---

[9] Maintaining control over access is the most significant factor in insuring technical security, according to the technical services personnel who are responsible for conducting electronic sweeps at the Bureau. Much of the effort of the new Security Division has been focused on ensuring that access to secure areas and SCIFs is controlled according to applicable inter-agency requirements. In addition, efforts to focus authority for security programs within a central office at major FBI facilities, help provide the senior executive with a consistent and appropriate security response. For example, physical security at FBI facilities in Quantico, Virginia, are to be consolidated under a single security professional who reports to the senior executive responsible for those facilities.

[10] The first part of this sentence is a paraphrase of a quote from J. Edgar Hoover on the courtyard wall at FBI Headquarters.

personnel at facility entry points and by card readers and alarms for secure areas.

Document control, like most FBI work, currently revolves around the case. Opening a case in response to a crime is a means for organizing record control. Access and need-to-know provide some basis for making decisions. Under the new demand for a more proactive and perhaps pre-emptive FBI capability, what will take the place of the case? Certainly the intelligence community could offer models for centering and focusing work processes, but they may not be the best ways for the FBI to organize. There are other organizations organized around public safety concerns, and they may provide some insight. The challenge for the FBI will be to preserve its ability to cooperate with a diverse set of organizations without an investigative case being opened.

Since documents are in many ways the means for moving cases forward - and because the FBI, more so than many government organizations, remains a culture of paper - how they are handled can dramatically affect the efficiency of FBI work. The tension between securing and sharing information arises directly. For law enforcement, the motto is what you don't know could kill you. Before following a lead or proceeding with a line of questioning, an agent will want to know as much as possible about the people and organizations with which he or she will come in contact. For a security professional, the challenge is to strike a balance between wide versus narrow access to information, all the more so when the bulk of classified documents handled by the Bureau originate outside the FBI.

Documents often come with specific rules that govern where documents may be viewed, what can be reproduced, and how they can be transported outside the facility in question. In some cases, the FBI does not have control over who is on the distribution list, and the Bureau may be restricted from sharing information with anyone outside the Bureau. Within these requirements FBI work is accomplished. The need to share information among FBI-hosted Joint Task Forces may dictate

how members are selected, vetted, and detailed from their home organizations. Otherwise, sensitive information may not be available to the Task Force or available to only a few FBI employees on the Task Force.

In this type of environment, the most important part of document security is trust and confidence in the security procedures and practices that certify personnel and control access. Document security at the lowest level must rely on the professionalism and attention to detail of each FBI employee. Those officials need procedures that are clear and uncomplicated. They need effective means for storing and working with documents that help them protect a document and enable them to control access. These practices need to be evenly applied from the top to the lowest level within the Bureau. Exceptions need to be the result of a deliberate process, one grounded in mission success and well thought out.

AREAS OF ONGOING IMPROVEMENT

Better Access Control

Since the 1995 bombing of the federal office building in Oklahoma City, the FBI police that guard the J. Edgar Hoover building and the Bureau's Field Office in Washington, D.C., as well as its facilities in Quantico, Virginia, have gone to 12-hour shifts. This has helped to ensure round-the-clock protection of key installations. Admission to FBI facilities for both vehicles and individuals is more tightly controlled now, especially following the September 11 attacks. In addition, the FBI has budgeted for and begun to install intrusion detection devices at all of its facilities throughout the United States. In principle, this means that alarm systems will be placed at each and every FBI facility. Once in place, each Field Office will be able to monitor these anti-intrusion systems for every facility in the office's territory.

The use of card readers and other access controls has increased to provide better accounting of physical access to secure and other sensitive areas (for instance, armories). This improvement has been driven by the growing reliance on protected information under national intelligence programs for CT and CI case work in Bureau Field Offices. The number of internal SCIFs (Sensitive Compartmentalized Information Facilities) has risen dramatically in the last three years. Accrediting SCIFs is a primary duty of the Security Division, but SD works with individual Field Office security officers to develop and accomplish it. Card readers can assist in maintaining internal security for offices that have a large number of non-FBI personnel working in the facility. It is possible to identify specific rooms and areas where only designated work groups have unescorted access. This relies on each cleared person taking assertive action to challenge non-cleared personnel and requires appropriate IT safeguards to insure that physical access and system assess are the same.

One Security Division program documents and manages vendor clearances and certification. It monitors vendor paperwork and helps enforce access controls. There is a deliberate methodology for determining when vendors and contractors do not need escorted access. This process looks at the sensitivity of the work to be performed, need for regular access, and nature of the tasks. Once a vendor or contractor has been entered into the FBI database, all FBI facilities have access to the data. Personnel working under vendor or contractor agreements are subjected to the same process and also are displayed in the database. Material being delivered to headquarters must first go to an FBI off-site warehouse or be certified by that facility.[11] This helps control and manage the threat posed by external introduction of electronic devices. Once there is a better understanding of the threat within the United States, a similar program may need to be instituted for FBI facilities worldwide!

[11] Vendor certification is maintained for all FBI facilities by a central Security Division database.

Offices where steps have been taken to professionalize the security function fare better at securing work group acceptance. They extend what had been an administrative function to a broader responsibility for mission security. In large Field Offices these centers have evolved into control centers with a duty Agent who not only helps facilitate police and security responses to office alarms, but also serves as a means for quickly responding to a crisis. By contrast, there is some indication that where the security function is still considered an administrative function, the facility control center may not be manned around the clock. At a minimum, a more professional security operation leads to a better understanding of secure area and SCIF accreditation standards and a more robust administration of document control. Centralizing policy for this area within the Security Division helps to standardize FBI procedures and provide a single authority for adapting standards to the Bureau's work processes or those of Joint Task Forces. Given the Director's support, it also signals the Field Offices that physical and technical security rank high among the FBI leadership's priorities.

Improved Security of Documents

The Webster Commission endorsed the document control systems created, in particular, by the Central Intelligence Agency. In effect, the commission urged that the FBI adopt that agency's methods and procedures for securing documents, and for the most part this still is a valid recommendation. Following the arrest of Hansen and completion of the Webster Commission's investigation, the FBI did strengthen significantly its handling procedures for classified documents. Security officers in Field Offices, whose work had focused on administering personnel security, were told to review and insure that procedures for recording access and maintaining positive control were being followed. The need for new SCIFs and other sensitive areas also drove more agents and employees toward the security officers, who helped guide physical space requirements and build checklists and access

rosters. All FBI personnel who need a card reader or certified lock for storage of classified material now can go to the Security Division for such equipment. This gives the SD more control of overall document handling at Field Offices and other work centers in the Bureau. Awareness has grown throughout the Bureau of how important it is to treat such documents properly, and so has the willingness to ensure their security through a policy of zero tolerance of any leaks.

SUGGESTIONS

Provide More Pay and Flexibility to FBI Police

The 12-hour, 60-hours-per-week shifts being pulled by FBI police in the Washington area for the past seven years constitute a problem in search of a crisis. The Bureau is finding it hard to attract and retain sufficient numbers of qualified personnel. The current threat assessment also requires additional manpower for personnel and vehicle inspections, and other tasks associated with an increased level of vigilance in and around FBI facilities. Especially after September 11, the nationwide demand for police personnel has increased dramatically, not least within the federal government. One of the FBI's greatest competitors for trained personnel, in fact, is the Air Marshall program, which was expanded by Congress after the terrorist attacks and which can outbid the Bureau for well-trained police. It draws a significant number from the ranks of FBI police, who have suffered from the long hours (notwithstanding overtime pay), as well as lower base salaries. Other federal police programs have greater authority over pay, thus providing them more flexibility in attracting and keeping trained personnel.

In these circumstances, increasing the base salary paid to FBI police and providing increased flexibility would help the FBI retain a police force with a reasonable level of experience. It would help stem the outflow of police to higher paying jobs and perhaps also increase the number of new recruits, thus enabling the police force to operate on

a more normal 8-hour, 40 hour week, shifts. An additional benefit would be more time available for in-service training of police. The time available for training is short at present because of the increased demand for police coverage on patrol and the short supply of manpower. Placing the police under the control of a security professional at each level in the Bureau would help to centralize formal authority for security and provide the senior executive at each level with a single point of contact for security matters.[12]

In the headquarters and at Quantico facilities, non-armed security personnel also suffer from a lack of manpower to perform internal building security patrols. The teams are limited to merely checking that corridor doors are locked and coffee pots are turned off. Essentially a cursory security and fire safety patrol, they do not enter secure areas to check that material is secured after hours. If an internal alarm is activated, they work with the police to investigate the alarm and maintain custody of the space until it is secured. Additional personnel would allow them to start looking for instances of unsecured materials and poor office discipline to head off potential security incidents.

Implement Entry/Exit Checks on Documents

In the near future, the Bureau should move quickly, as the Webster Commission suggested, to establish a system to check for classified and other sensitive documents being carried out of FBI facilities by anyone. In a world where a single compact disc can contain more information than a hostile intelligence service could process in a year, such a system will need to be carefully shaped or it will become a large nuisance with a minor effect. Some spot checking could serve as both a reminder and a deterrent. Having officers log out classified material that is being removed would reinforce security procedures.

---

[12] While this study was underway, FBI police at Quantico were placed under the control of a security professional.

Document security programs need to be fully implemented within the Bureau and better funded. With the Joint Task Forces spawned by the war on terrorism, exceptions have now become more common. The requirement to clear non-FBI personnel into FBI workspace creates a demand on security personnel who process outside personnel, as well as on those conducting background checks. This is a consequence of doing business using classified information in FBI workspaces and it needs to be programmed and budgeted sufficiently so that operations are not constrained. And the individuals being granted access need to be recorded and properly briefed/debriefed.

Examine New Ways of Standing Up Task Forces

As "need-to-know" is rethought and implemented Bureau-wide, the FBI should explore alternate ways of standing up Joint Task Forces. Placing documents on the FBINet without more stringent profiles and accountability procedures cuts against the individual agent's responsibility to be aware of who has access to his or her information. Other models are suggestive. In the NATO alliance, for instance, national information is either vetted for the alliance or is walked into the system via a few trusted agents who can then act on it within the context of their work on behalf of the alliance. In another model, a trusted agent sits outside the work group with access to documents within and outside the workgroup. He or she prepares tear-line type products or is in a position to open access based on an operational need. More work needs to be done to insure that the FBI's mission can be enabled by workable document control and vetting procedures. It will be necessary to improve the collaboration with other government agencies and organizations that control classified information to ensure that work processes remain mission oriented while protecting documents.

Rethink Policies toward Wireless Communications

In large part because the technical security mission is split between at least two major FBI divisions and is focused on missions and facilities outside the United States, the bulk of FBI middle to senior agents and support personnel have received little training on the nature of technical threats. Cell phone and wireless LAN technologies such as 802.11b (Wi-Fi) are naturals for improving the sharing of information in the Bureau's culture, but the security risks of such devices are not well understood by FBI personnel.[13] For instance, recent plans to create a wireless LAN at Headquarters or place cell phone antennas within FBI secure areas were caught only at the last minute by technically-trained agents and security officials.

Security officials need to develop a deliberate process for determining the threat and, once that has been done, educate FBI personnel on the threat and the consequence of using specific technologies in their work processes. The goal should be to develop an aware user who employs technology in an appropriate way with as little disruption in work patterns as possible. Technically-trained agents (TTAs) are the FBI's most significant technical experts, with credibility in the field on technology issues, but even they do not always have the most up-to-date information on the risks of misusing technology in FBI casework - for instance, keeping cell phones turned on or failing to separate them from their batteries inside an FBI facility. TTAs receive some in-service training, but rarely does it include

[13] We found cell phone usage quite high in areas like New York where public telephones are difficult to find in working order. (A recent order by the AD required all cell phones to be turned off when in a FBI workspace.) In addition, the more open attitude and approach that may be present in Joint Task Force work areas create an environment where electronic devices may be used increasingly. Generally, Joint Task Forces working on a crisis or an issue like counterterrorism do not have desks, secure telephones, and computers for everyone assigned to the work group. This creates a demand on the limited supply, and cell phones and shared computers fill that demand, becoming a necessary part of the work process. This situation also creates an opportunity for an offensive attack on the workspace that has to be balanced with the need to share and use the more open devices.

updates on technical security threats and the potential problems presented by rapidly evolving consumer technology.

Work with ITD in Developing a Technical Research Program

Technical security is a policy issue for the Security Division, but SD also depends on the expertise of the Investigative Technologies Division.[14] As a result, the two need to collaborate in defining new polices and practices for technical security. During a transition period, it may be necessary to create a joint policy board or some other structure to reflect the perspectives of both disciplines, thus helping to ensure that the very capable technical services currently provided to the field continue in the new security context. There is a business agreement linking the technical functions formally in the Laboratory Division and the Security Division, which seems a reasonable first step toward harmonizing both efforts.

Part of this collaboration should be a technical research program that looks at emerging technologies and the FBI's approach to work - to identify technologies that could be useful to FBI agents and support teams. This research program would try to leverage other interagency research, but it would focus resources on specific FBI work processes and problems. For instance, there are pockets of excellence within the FBI that contribute to the protection of FBI secure areas and SCIFs, within the United States and especially abroad. Budgets were allowed to decline, but recent corrections have started the trend upward since the Webster Report came out. These technical abilities need to be enhanced

[14] The Investigative Technologies Division traditionally was focused on supporting national security and overseas work by the Bureau. Very few had any recent experience working with FBI FO agents on technical security matters. One could point to some incidents requiring them to deal with internal technical security threats, but not to systemic methods for determining such threats. Likewise, very little time is spent in training new agents about technical security and the consequences of not following what could be termed *operational security* procedures and techniques. TTAs do get some additional training, but again there is little understanding of the threat to domestic FBI operations.

with a robust research and development effort that looks at new technology within the FBI agent work context.

Having a closed intra-FBI network helps but does not eliminate the technical security problem. Again, SD should invest in research programs that help define the threat and help prepare the Bureau to meet emerging technical requirements to protect documents and information. Likewise, when new technology becomes available, security must act quickly to determine how it can be used in the field. Otherwise, FBI officials will take the lead in employing the new technology without being fully informed as to the consequence of such use.

Better Define and Train Technical Security Processes

Clearly, technical security processes need to be better defined. Everything from vendor certification to technology use needs to be properly vetted with a technical services unit tasked by security to determine appropriate use. It is difficult for security customers to determine where they need to go to gain approval for a specific electronic device if it is not already certified. Likewise, cell phones and wireless LAN technologies such as 802.11b (Wi-Fi) need to be reviewed so that use does not conflict with secure area requirements. Currently, all FBI space is considered secure space. A systemic look at the technical threat by the Security division will help ensure that any entry into FBI space receives an appropriate level of attention, inspection, and control.

Operations and technical security topics need to be incorporated into entry, mid-career, and leadership training programs. In addition, as security officers become more professional they need specific training on technical subjects and FBI procedures for handling them. They need to be made more aware of the technical security problem so that they can help guide field leadership in the management of their facilities and work processes. Each security officer needs to be more

aware of the consequences of technology use so that his or her guidance can be incorporated into agent and office best practices.

Finally, there is no substitute for consistency by leadership at headquarters and in the Field Offices in applying restrictions on the use of technology and granting access to secure and sensitive areas under FBI control. Consistent, even application will help strengthen those employees adapting their work practices to best practices. It will enhance the ability of the institution to provide a safe and secure work environment. Likewise, technical and security officers concerned with technical security policy must be sensitive to work demands of FBI personnel and find ways to meet mission requirements within the security guidelines of the Bureau.

V. CONCLUDING OBSERVATIONS

The FBI security program has made notable progress in the last two years. While responding to September 11 has dominated everything the Bureau has done, the security program is being implemented with dedication and enthusiasm. Most importantly, there appears to be a senior leadership commitment to make security a key concern of FBI operations and support programs. In addition, the newly created Security Division (SD) team is stepping in the right direction to implement comprehensive reforms that place security within the fabric of FBI culture.

DEVELOPING POLICY

It was not possible with the information available to do even rough assessments of the adequacy of time and resources Bureau's security program, but the recent program/project management initiatives seem on the right track. Engaging MITRE, a top-flight systems consultant, and creating a team to look at project and program management should provide more reach and coherence while taking some of the pressure off already over-burdened senior managers. Any efforts to increase buy-in by section and unit chiefs is welcome, as are any efforts to sort contemplated actions into projects and to begin to make priorities among those projects. The next steps - to look at what is missing, and to evaluate budgets in light of priorities - should provide the wherewithal for the kind of assessment that was contemplated in task 4.

The process then intends to develop metrics for assessing implementation, and thus to give SD senior manager a way to look across all projects and programs. That, too, surely seems all to the good, though what has been done so far illustrates just how hard it is to connect specific actions to broader objectives, let along to measure their success. The goal of an enterprise architecture for the Security

Division likewise seems appropriate. Again, the test will be in the doing.

It is still early in the security policy process, and the obstacles ahead are formidable. As we note in several places in this report, and as the FBI Security Program Plan clearly acknowledges, many policy decisions of major importance remain to be made. Thus, it is too early to make judgments about the adequacy of future resource commitments to security; they can be judged when major policy decisions and more concrete implementing plans are in place. There is no need to belabor the point, but a few examples from our assessment and from the Security Division Program plan will make it vivid.

There is no quantitative description of what has to be done, and no estimate of the resources that will be devoted. There are some (classified) 2003 budget numbers, but they are not put against any tasks that are adequately described for cost analysis; there is no indication of whether these are the entire security-related budget; and they are not put in the context of the overall budget.

Indeed, in the Security Program Plan (hereafter SPP) talks more about needs than actual resources. For instance, (emphasis added):

''The Security Division will ensure adequate staffing is maintained to support both the investigative and adjudication components of the process. (p. 24)''

''…the Security Division will be dependent on the following factors:

- …
- Funding for security awareness training and education.
- …
- Sufficient personnel resources within the Personnel Security Section…
- Sufficient base funding… (p.32)''

''In five years, the Security Division envisions the FBI transitioning into an organization in which security is considered a core function and is recognized for its value-added to operations and personal safety. (p. 19)'' On its face, five years seems like a reasonable schedule to accomplish all that has to be accomplished, assuming the resources are available. But, again, a more useful assessment cannot be made without knowing more of the specific policies and plans called for in the SPP but not yet in place.

The metrics of pages 39-40 would be a useful starting place for a resource adequacy assessment if there were resource estimates stacked up against them. Right now they are only for FY 2003 so they would obviously have to be extended across the entire five-year plan, which also seems about the right horizon for resource planning. The metrics only call for ''20 percent'' of the ''security risk analysis capability in the final Security Division structure'' to be operational in that year, which raises the question of whether it might not be possible to do better.

None of the metrics deal with attributes like employees screened, the security of information systems, or the state of physical and technical security. They are about getting SD organized and staffed, and thus are aimed at a high-level audience. Each section is then to draft a more detailed plan.

One thing that does seem missing is any plan for a serious ''Red Team'' effort to try to break through existing security. This should be a part of the plan, separately organized and funded. Related to this, the fourth of the ''priority performance gaps'' noted on page 15 was ''Security programs are not adequately addressed to determine the effectiveness of targeted programs.'' This point is downplayed it the rest of the report, mentioned in passing as part of SD-G2 on page 17, at the bottom of page 20, and in reference to current policies on page 21.

We would recommend that a major specific part of the SPP be a plan for policy effectiveness assessment, and the resources to do it.

THE STAKES IN DECISIONS

It is worth stressing again that in all three areas of security, but especially in the IA realm, policy decisions cannot be made by SD alone. They involve equities that run well beyond security. In particular, the Bureau is making a very large investment in Trilogy, a new information system. The security structure of Trilogy will affect how the Bureau approaches its work processes - how both criminal case and national security-derived information are shared. The longer decisions bearing on security policy are put off, the more likely it is that Trilogy will not adequately embody required security qualities.

If security is to be balanced with - ideally become a facilitator of - more effective work processes, decisions will have to involve the senior leadership of the Bureau. Left alone, security becomes a special pleader, and the likely result is decisions that are lose-lose, ones that do not enhance security as much as it necessary but are seen, perhaps wrongly, as just more rules, more obstacles to getting the job done.

The SPP speaks plainly of security-related functions, such as Field Office physical security (run by SACs) and ''elements of'' communications and technical security (run by ITD) that are outside of SD. Indeed, section F of the SPP, ''Dependencies, Obstacles, Mitigating Factors'' is remarkably candid about the organizational challenges the SD faces in general, especially in working with all the other divisions. The section is also remarkably candid about the more mundane immediate problems they are having, like getting office space and enough new employees. These are not ''resource'' problems in the classic sense. More money is not the primary answer; more streamlined procedures is, if there is one.

Security both affects and is affected by work process. Security need not be the enemy of efficiency, for instance in sharing information, but it often appears that way. At worst, if security programs appear to be external to the core functions of the organization, security can become isolated from just the operational processes it seeks to affect.

Likewise, workspace technical security issues will affect where and how people work. In the past, these issues have been centered in counterintelligence (CI) and national security programs or overseas areas, but in today's highly technological public environment they can affect all FBI operations and support. In addition, the FBI intranet (the FBINet) operates at the SECRET level, which carries consequences for access and equipment that shape individual squad work processes whether they are working on counterterrorism, other national security or criminal casework.

These issues bear particularly on how material will be handled within FBI-hosted Joint Task Forces (JTFs) that include personnel from a range of federal and local government organizations. Security policies that affect access to FBI space and networks will be either be enabling or constraining of work processes. What is needed is a deliberate security process that focuses on facilitating FBI operations while maintaining clear work group control over access. This process crosses the full range of security policy from personnel vetting and suitability, to physical access to FBI space and work centers, to document control and information management.

CHANGING ORGANIZATIONAL CULTURE

Reinforcing security at the Bureau amounts to a major change in organizational culture, one that is occurring at the same time as the Bureau is reshaping its mission. The change is visible; Field Offices that a year ago let security reinvestigations lag as low priority

business now call in advance to get next month's roster of those who are up for reinvestigation. We also found added emphasis in getting security input early when offices are contemplating moving or doing construction. There is a greater awareness that security, like other enablers such as safety, should be intrinsic to all operations and support, part of FBI best practices and agent tradecraft. Security is not just about protecting national security information. It is about being smart, and gaining operational efficiencies as it seeks protection for FBI knowledge, facilities, and people. To be sure, the FBI had, and still has, a long way to go; that is particularly the case for information security, where specific shortcomings are rooted in the woeful condition of the Bureau's information technology (IT) more generally.

Most of what has been accomplished can be attributed to the security structure provided by senior leadership as a consequence of creating a Security Division. That creation brought a cadre of security-minded officials drawn, in many cases, from agencies and offices within the intelligence community and dedicated to a ''never again'' set of goals. They brought rigor and a process for meeting internal and external security tasks. It centered security policy at an appropriate senior level, helping with implementation and providing the Director with a senior advisor on security matters. (Something similar probably needs to be replicated at the Field Office level to gain the same centralization over policy execution and again provide the senior executive in the Field Office with a professional security advisor.)

However, security cannot be imposed from outside the Bureau. To be effective, it must come from within and be pushed by internal groups with operational credibility. Security issues need proponents within the training and operational culture of the FBI. While there is a security presence during initial agent training, it is modest, and while opportunities to discuss security issues with mid-career personnel are increasing, they remain few. Without more opportunities for educating agents and support personnel, the process for balancing security with

operational necessity will lack the operational push-back that is needed.

Several challenges run across the entire FBI security program:

·Professionalizing the Bureau's security operations - as well as the larger information technology (IT) structure in which they are embedded. This is very much a part of the current program. Given the relatively low priority of security, work in the area has not been a profession. It is, for most at headquarters especially, a collateral duty, not a primary one. The duties of security officers have been mostly administrative, revolving around personnel security paperwork. Security officers have not generally been asked to be, and are not, proactive. The intention to create a cadre of security professionals, including special agents but also non-agents, surely is the right one. The questions here are resources and the role of agents in an agent-dominated culture.

·Institutionalizing "need-to-know." For reasons deeply rooted in the Bureau culture and in law enforcement, "need to know" was not really applied, and in many ways was not really thought through. Robert Hanssen continued to have access to information when he no longer had a valid need to know. Likewise, local law enforcement personnel detailed to a Bureau-hosted Joint Terrorism Task Force probably do not have a need-to-know when it comes to criminal corruption cases. The issues here are how to institutionalize need-to-know while impeding as little as possible the free internal flow of information that has been the hallmark of the Bureau's law enforcement culture.

·Making threat assessments more systematic. At present, threat assessments seem to be made in a mostly *ad hoc* manner. How should the threat be conceived, when non-state actors - ranging from organized crime, through rich swindlers, to terrorists - are now more threatening? In the investigations area, for instance, there seems the most concern

about new hires, especially translators, born abroad and now in mid-life. That seems fair enough, but whence does it derive? Some mechanism for more systematic threat assessment seems necessary, both to guide the security program generally and with respect to specific systems.

·Recasting squad and support group work processes within the new security environment. Current work processes hinge on opening a case in response to a crime. A case provides the context for gathering information, assigning investigation tasks, and even assigning need-to-know. Yet, as the Bureau's mission shifts from law enforcement toward prevention, from reaction toward pro-action, the case model may not support all FBI missions. Terrorist groups, for instance, might only commit a crime at the end of a long chain of activity, so working proactively against them means looking at predictive criminal behaviors within an information-intensive environment. The security foundation required will be different from that for case-driven law enforcement.

·Harmonizing new technology to work smarter with technical security concerns about information and personnel. Careless cell phone practice, for example, not only puts at risk operational information but may also allow a technologically aware adversary to track a user's position. While today this may be mostly a risk overseas, the risk of compromising a domestic operation is present. At one level, this means that security must balance risk with deliberate process. At another level, it means that the technical security input must have credibility with core work groups lest those groups ignore or work around security directives. This may also require the Bureau security effort to invest in research to best leverage technology within an operational context, and it will dictate a renewed commitment to technical security education and training at the entry and in-service levels.

·Revising the operating manuals (Manual of Investigative Operations and Guidelines, MIOG and, Manual of Administrative Operations and

Procedures, MAOP). This would seem minor but has more than minor implications. Because major parts of the manuals are so out of date, when the Field Offices (FOs) are inspected, they get penalized for security violations that no longer matter much, while more serious concerns go unnoticed. The poor focus trivializes what should be an important process. It also penalizes the security officers while letting supervisory special agents off the hook.

There are no absolute guarantees in the security business. And rightly so, for security is not the business for the FBI or most other organizations. Instead, the overarching security goal, in the language of FBI security managers, is to reduce the time from ''defection to detection'' and to do so with as little cost to the efficiency of ongoing operations as possible. Security also means a commitment to building a safer and more secure work process. The agent, squad and support personnel are the basic implementers. The intelligence agency template for security - which underlies both the Webster Commission report and the current security program - will have to be adapted to meet the needs of an evolving organization whose traditional law enforcement mission will remain important and whose upgraded counterterrorism mission will be preoccupying.

In that sense, the buy-in that is most crucial is not SD section and unit chiefs, though they are critical. Rather, it is FBI officials beyond security. To say they need to be involved at each stage in the process is easy for us to say but hard for SD to accomplish, all the more so given the demands on the leaders' time and attention, as well as those on the entire Bureau as it seeks to reshape its mission. So far, SD managers have been perceived as sensitive to the FBI culture. The challenge looking forward is to make Bureau officers into partners in both recognizing the importance of security and working to make it an enhancer of performance, not an obstacle. While the metaphor of "Webster versus 9-11" is entirely understandable, the FBI security program will be a success when that metaphor no long seems appropriate, when security is taken as part of the natural work process, not

something that adds to or competes with getting the Bureau's critical work done.