July 2005
Volume 74
Number 7

**United States
Department of Justice
Federal Bureau of Investigation
Washington, DC 20535-0001**

**Robert S. Mueller III
Director**

The *FBI Law Enforcement Bulletin* (ISSN-0014-5688) is published monthly by the Federal Bureau of Investigation, 935 Pennsylvania Avenue, N.W., Washington, D.C. 20535-0001. Periodicals postage paid at Washington, D.C., and additional mailing offices. Postmaster: Send address changes to Editor, *FBI Law Enforcement Bulletin*, FBI Academy, Madison Building, Room 201, Quantico, VA 22135.

This publication is produced by members of the Law Enforcement Communication Unit, Training and Development Division.

Internet Address
leb@fbiacademy.edu

Cover Photo
© Digital Juice

Send article submissions to Editor, *FBI Law Enforcement Bulletin*, FBI Academy, Madison Building, Room 201, Quantico, VA 22135.

FBI Law Enforcement Bulletin

Features

Departments

ISSN 0014-5688 USPS 383-310

Risk Assessments and Future Challenges

By W. DEAN LEE, Ph.D.

By recognizing existing and emerging threats, law enforcement agencies can improve their risk assessment and management programs. Too often, for example, security risk assessments focus mostly on identifying flaws in physical security (e.g., perimeter barriers and screening visitors) without fully recognizing the impact of other security challenges (e.g., internal people problems and cyberthreats). Applying a systematic approach of fact finding and balancing costs and benefits should lead to better security and operational decision making.

The analytical risk management (ARM) process is a systematic and interactive approach for identifying and evaluating assets, potential threats, and existing vulnerabilities, along with calculating risks and determining requisite countermeasures.[1] Departments can view the ARM process as three interacting spheres of assets, threats, and vulnerabilities. Where these three areas merge, or overlap, are the calculated risks. Once a department's risk managers determine the risks, then they can select appropriate countermeasure options to mitigate them. Most important, ARM can service both security and operational assessments.

The ARM process expresses risk, defined as the potential destruction, disruption, or denial of essential assets, in the formula Risk = Impact of Loss of Asset x Threat x Vulnerability or R = I x T x V. In other words, a risk assessment (R) determines the possibility of an adversary's (T) successful

> ***"Applying a systematic approach of fact finding and balancing costs and benefits should lead to better security and operational decision making."***

Dr. Lee, the architect of the FBI's Security Risk Management Program and Continuity Assurance Planning Strategy, leads the Bureau's Security Risk Analysis Staff.

exploitation of an identified vulnerability (V) and the resulting degree of damage or impact (I) on the asset. Basically, risk management constitutes the continuing process of selecting and applying explicit countermeasures to achieve optimum results while balancing acceptable risks and costs. By developing a full-spectrum risk assessment and management program, a department can discover its security and operational strengths and weaknesses. In addition, it can determine how best to maximize asset usage.

ASSETS

For the ARM process, assets comprise resources of essential value that a department must protect to effectively fulfill its essential public safety and law enforcement responsibilities, a definition that differs from that traditionally used in law enforcement and intelligence circles. Assets include people, information, operations, equipment, facilities, and social-psychological resources (PIOEFS).

Assessing assets involves three sequential actions. First, a department's risk managers identify all important local organizational and operational PIOEFS resources requiring protection. Second, they write a brief statement for each describing the worst undesirable event should some adverse situation affect that asset. For example, within the people category, a department should include law enforcement officers as a critical asset, and an applicable undesirable event would be criminals or terrorists attacking with improvised explosive devices that could result in the loss or injury of the officers.

Third, the risk managers assign a linguistic rating (value/criticality) to each asset based on the impact of loss or damage. This means that risk mangers first assess an asset according to one of the four defined *criticality* ratings of critical, high, medium, and low and then further refine the resource into three *values* of low, medium, or high.

- Critical: grave effects leading to loss of life, serious injury, or mission failure.
- High: serious effects resulting in loss of highly sensitive resources that would impair operations affecting public safety and community interests for an extended period of time.
- Medium: moderate effects resulting in loss of sensitive resources that could impair operations affecting public safety and community interests for a limited period of time.
- Low: little or no effects impacting human life or the continuation of operations affecting public safety and community interests.

In the example of officers as a critical asset, the department might assign an impact rating of low/critical, meaning that it deemed the resource as overall critical but at the lower end of that category. Finally, the risk managers convert the linguistic

ratings into numeric impact values. The numeric value will be impact (I) in the equation I x T x V = R. Chart 1 and Table A illustrate this process.

THREATS

Threats are general situations with the potential to cause loss or harm to essential assets, whereas adversaries constitute specific hostile individuals or groups with the intentions, capabilities, and histories to conduct detrimental activities against law enforcement agencies and public safety. Conventional external threats involve individuals, domestic groups, and sometimes foreign entities. Individual dangers include street criminals of varying sophistication; computer hackers intent on penetrating, stealing, altering, controlling, or deleting law enforcement data; insiders, such as corrupt officers, supervisors, and administrators; and people with personal, emotional, or psychiatric crises. Group threats can involve regional and international organized crime figures; left-wing, right-wing, and special interest extremists; and foreign, domestic, and transnational terrorists. Foreign perils can comprise foreign intelligence services masquerading as business persons, visiting delegations, false-front companies, travelers, journalists, scientists, students, and diplomats; state-sponsored entities attempting to influence the American public through the media and select organizations and to acquire U.S. research and development technology; and foreign economic menaces endeavoring to control U.S. industrial, banking, and commercial interests.

Assessing threats involves identifying and assessing all of the threats associated with each asset. For example, law enforcement officers might face two main street hazards: criminals and irate citizens. First, a department identifies the specific potential adversaries for each threat. Criminal adversaries could include local street gangs and organized crime figures, whereas irate citizens could comprise spouses engaged in chronic and escalating domestic violence. Next, the risk managers write a brief statement highlighting each adversary's intent, capability, and history of violence. Then, they assign a linguistic rating (value/criticality) to each danger based on the adversary's overall intent, capability, and history. The risk managers assess a threat according to one of the following four defined *criticality* ratings and then further refine it into three *values* of low, medium, or high. The definitions for threats differ greatly from those for assets and vulnerabilities.

- Critical: a definite danger as the adversary has both the intent and capability to

Common Threats Facing Law Enforcement Agencies

- Criminal: menacing, assaults, vandalism, thefts, arson, and computer hacking
- Natural: fires, floods, power failures, and storms
- Domestic: civil disturbances and special event problems
- Terrorist: bombings, sabotage, hostage taking, kidnappings, and homicides
- Internal: corrupt officers, misuse of authority or resources, and malicious acts by disgruntled workers

Chart 1 - Asset Assessment Example

Critical Asset	*UDE Code*	*Undesirable Event (UDE)*	*Linguistic Impact Rating Degree / Criticality*	*Numeric Impact Value*
People				
(P-1) Departmental Personnel (full-time officers, auxiliaries, JTF members, technicians, & administrators).	P1A	Terrorist or criminal attacks (e.g., vehicle & package IEDs, hazardous mail, & physical assaults) causing loss of LEA lives.	Low / High	14
	P1B	*(Insert additional items & blank lines as needed).*		
Information				
(I-1) LEA sensitive information in various media.	I1A	Internal & external thefts compromising law enforcement sensitive resources & operations.	Medium / Medium	5
Operations				
(O-1) Ongoing investigations & operations.	O1A	Detection of LEA UC operations causing loss of lives, CI assets, and jeopardize officers and cases.	High / High	49
	O1B	Improper security discipline and security lapses causing compromised operations	Low / Critical	50
Equipment				
(E-1) Communication devices.	E1A	Loss of electrical power or communications causing disruptions of operations.	High / High	49
(E-2) Weapons, ammunition, radios, & specialized gear.	E2B	Thefts causing loss of weapons, radios, & equipment.	Medium / Critical	71
Facilities				
(F-1) Main Headquarters & substations	F1A	Unrestricted publicly accessible pathways in adjacent property causing penetrations and attacks.	Low / Critical	50
Socio-Psychological				
(S-1) Community public relations.	M1A	Loss of public trust and community support may result in increased crimes.	Medium / Critical	71

Conversion Table A (Assets & Risks)

Low			Medium			High			Critical		
L/L	M/L	H/L	L/M	M/M	H/M	L/H	M/H	H/H	L/C	M/C	H/C
1	2	3	4	4	5	13	25	49	50	71	100

For converting linguistic ratings into numeric impact values for assets and for converting numeric values into linguistic ratings for risks.

launch an assault and a history of conducting similar incidents.

- High: a credible danger as the adversary has either the intent or capability to launch an assault and a history of conducting similar incidents.
- Medium: a potential danger as the adversary has the intent and the potential to receive the capability through a third party to launch an assault and has a history of similar incidents.
- Low: little or no credible evidence of the adversary's intent or capability to launch an assault and no history of conducting similar incidents.

In the example of street gangs as a threat, the department might assign a threat rating of medium/critical, meaning that a department considers the threat as overall critical and at the center of the category. Finally, the risk managers convert the linguistic ratings into numeric threat values and record the results for each identified adversary. The numeric value will be threat (T) in the equation I x T x V = R. Table B and Chart 2 illustrate this process.

VULNERABILITIES

Vulnerabilities represent weaknesses that an adversary can exploit to gain access to an asset. In essence, vulnerabilities are pathways leading to PIOEFS assets that include people, information and information systems, operational procedures and personnel practices, equipment characteristics, facility locations and building features, and social-psychological weaknesses.

> ***"Vulnerabilities represent weaknesses that an adversary can exploit to gain access to an asset."***

Assessing vulnerabilities involves first identifying the specific potential weaknesses for each asset. For example, law enforcement officers might experience human temptations to misbehave or become hampered by obsolete departmental policies and procedures. Next, the risk managers determine the existing countermeasures for each asset and their level of effectiveness in reducing vulnerabilities. Then, the risk managers assign a linguistic rating (value/criticality) for each according to one of the following four defined *criticality* ratings and further refine the vulnerability into three *values* of low, medium, or high, which differ significantly from those for assessing assets and threats.

- Critical: no effective countermeasures currently are in place, and known adversaries would be capable of exploiting weaknesses to reach the asset.
- High: some effective countermeasures exist, but the asset has multiple weaknesses that adversaries could exploit to their advantage.
- Medium: some effective countermeasures exist, but the asset has at least one weakness that adversaries could exploit to their advantage.
- Low: multiple layers of effective countermeasures exist, and few or no known adversaries could exploit to their advantage.

Finally, the risk managers convert the linguistic ratings into numeric vulnerability values and record the results for each identified weakness. The numeric value will be vulnerability (V) in the equation I x T x V = R. Table B and Chart 3 present examples of this step.

RISK CALCULATION

Risk is the likelihood that an undesirable event will occur. By

Chart 2 - Threat Assessment Example

Critical Asset	*UDE Code*	*Threat Category*	*Adversary*	*Intent*	*Capability*	*History*	*Linguistic Threat Rating Degree / Criticality*	*Numeric Impact Value*
LEA personnel LEA information Active investigations Equip. & weapons HQ & sub-stations	P1A I1B O1A O1B	Criminals	Local & transient criminals	Street gangs ABC & XYZ intend to merge to attack police.	Gangs possess assorted weapons.	Six-year history of violence since arrest of T.J. Kooker.	Medium / Critical	.87
			Prisoners processing	Unpredictable intoxicated prisoners	Prisoners on PCP become powerful.	Weekend arrests are most dangerous.	High / High	.74
	I1A E2B S1A	Extremists	Terrorists, radicals, fundamenta lists	Left-wing & right-wing group intent on creating havoc during convention.	Both groups trained & equipped in civil disorder tactics.	Outside agitators arrive during major events.	Low / Critical	.75
	F1A F1B	Disoriented & displaced people	Deranged individuals	Mentally disturbed persons intent on self-harm.	Deranged people use multiple objects as weapons.	Problem patients released from county asylum.	Low / Medium	.25
			Transients, homeless, trespassers	Trespassers intent on stealing for money.	Transients capable of causing offenses.	Difficult trespassers since shelter closing.	Medium / High	.62

Conversion Table B (Threat and Vulnerabilities)

Low			Medium			High			Critical		
L/L	M/L	H/L	L/M	M/M	H/M	L/H	M/H	H/H	L/C	M/C	H/C
.01	.12	.24	.25	.37	.49	.50	.62	.74	.75	.87	1.00

For converting linguistic ratings into numeric threat values and for converting linguistic ratings into numeric vulnerability values.

calculating the risk, the department may obtain an estimate of the potential severity or outcome of an undesirable event. Calculating the risk for each identified asset involves recording the degree of impact relative to each asset (value of I), the probability of attack by a potential adversary (value of T), and the possibility of a vulnerability being exploited (value of V) and then multiplying I x T x V. After this, the risk managers would convert the numeric values into ratings and prioritize the risks based on findings, remembering that higher values indicate higher risks. Table A and Chart 4 illustrate this process.

COUNTERMEASURES

Countermeasures are actions taken to prevent, mitigate, or eliminate vulnerabilities and to enhance security or operations. Universal methods include improving training and awareness, modifying policies and procedures, practicing and enforcing discipline, controlling and monitoring accesses, installing new security or operational measures, improving overall conditions, and realigning efforts. Departments can identify and assess many potential countermeasures that they may use to reduce vulnerabilities by exploring as many solutions as possible; by developing a comprehensive strategy toward risk reduction; by discovering countermeasure

Chart 3 - Vulnerability Assessment Example

Critical Asset	*UDE Code*	*Vulnerability Description*	*Linguistic Vulnerability Rating Degree / Criticality*	*Numeric Impact Value*
People				
LEA personnel	P1A	Established daily routines & schedules of law enforcement officers & supervisors.	Low / Critical	.75
	P1A	Intimidations & physical assaults.	High / Critical	1.00
Information				
LEA information	I1B	Inadequate compliance to established security policies, programs, & procedures.	Low / Medium	.25
Operations				
Active investigations	O1B	Public building with inadequate monitoring, allowing penetration and exposure to investigations.	Medium / Medium	.37
	F1A	Operations center co-located in high-risk facility.	Medium / High	.62
Equipment				
Weapons, radios, & equipment	E1A	Inadequate radio communication systems.	High / High	.74
	E2B	Inadequate doors, locks, and alarms to properly safeguard contents.	Low / Medium	.25
Facilities				
Headquarters & substations	F1B	Presence of publicly accessible underground facilities (e.g., parking lots, loading docks, & fuel sites).	High / Critical	1.00
Socio-Psych				
Community PR programs	M1A	Insufficient public relations staffing and funding reduces positive contacts with the community.	High / High	.74

Chart 4 - Risk Assessment Example

Impact			*Threat*		*Vulnerability*		*Numeric Value*	*Linguistic Risk Rating Degree / Criticality*
	Rating	*Value*	*Rating*	*Value*	*Rating*	*Value*		
People								
Departmental personnel	L / H	14	M / C	.87	H / C	1.00	12.18	H / M
Information								
LEA sensitive information in various media	M / M	5	L / C	.75	L / M	.25	.94	L / L
Operations								
Ongoing LEA investigations	H / H	49	M / C	.87	M / M	.37	15.77	L / H
Equipment								
Communication devices	H / H	49	L / C	.75	H / H	.74	27.20	M/ H
Weapons, ammunition, radios, & equipment	M / C	71	L / C	.75	L / M	.25	13.31	H / M
Facilities								
Main Headquarters & Substations	L / C	50	M / H	.62	H / C	1.00	31.00	M / H
Socio-Psychological								
Community public relations programs	M / C	71	L / C	.75	H / H	.74	39.41	H / H

costs, including tangible training, additional personnel, materials, installation, operations, maintenance, and replacement requirements; by conducting cost-to-benefit analysis for each option and comparing appropriate alternatives; and by prioritizing options based on one or a combination of factors, such as cost, time, effort, organizational impact, resources available, and other specified criteria. Chart 5 presents an example and the following are universal countermeasure options to enhance the security of PIOEFS assets.

People

Members of the law enforcement community (e.g., officers, joint task force members, technicians, support personnel, administrators, and their families) comprise the primary asset. But, history has shown that some people also may pose prominent threats and vulnerabilities. The more people an organization employs, the higher the probability of more security and operational challenges. However, law enforcement agencies can mitigate people-generated problems by providing comprehensive indoctrination and recurring refresher training vital to proactively preventing violations, detecting abnormalities, and minimizing damages; by gaining positive leadership involvement and group support for all programs; and by scrutinizing all individuals who have direct and indirect access to essential PIOEFS assets.

Information

The increasing proliferation and circulation of large volumes of sensitive law enforcement data from multiple channels has grown progressively more

susceptible to exploitation by adversaries using human, electronic, and cyber-based means. To reduce these threats, departments should promote security awareness to decrease carelessness; identify and eliminate all known susceptible points of intercept in the communication network; and provide and enforce secure storage and proper disposal of accumulating information material, media devices, and sensitive trash.

Operations

Law enforcement operations, such as active investigations, security at high-profile events, and surveillance assignments, have become more geographically dispersed and increasingly reliant on computers and cellular communication connections, which then creates greater vulnerabilities for adversarial espionage and sabotage. Departments can lessen such dangers by inculcating operational security (OPSEC) early into all facets of individual daily affairs and special activities; enforcing strict need-to-know requirements; practicing OPSEC, especially at off-site and undercover locations; and integrating security compliance into all plans, policies, procedures, and performance reviews.

Equipment

Screening, accessing, and monitoring systems rapidly become obsolete in countering new and evolving multidimensional threats. To reduce security and operational failures, departments can integrate multiple resources to enhance security (e.g., physical barriers, electronic sensors, monitors, alarms, and human systems); program into future budgets the cumulative expenses for backup equipment, supplies, maintenance, repair, upgrades, and replacement systems; and exploit available off-the-shelf equipment to reduce internal research and development expenses.

> ***"By calculating the risk, the department may obtain an estimate of the potential severity or outcome of an undesirable event."***

Facilities

Centralized facilities and decentralized law enforcement activities present unique cooperative security and operational challenges. Departments can mitigate these by improving three-dimensional security perimeters with multiple rings and layers of mutually supporting protection; by assessing adjacent establishments as pathways for attacks and correcting gaps where possible; by protecting off-site locations with complementing security measures; and by providing separate visitor- and package-screening accommodations.

Social-Psychological Factors

Adversarial manipulations of public and organizational perceptions affect community support and internal morale. Departments may lessen social-psychological threats by recognizing the importance of community and individual concerns; by earning and preserving the public's trust and confidence; by understanding the impact of social, cultural, political, religious, and psychological influences in daily operational security practices; and by deterring, detecting, and defeating internal security and operational problems promptly and decisively.

RISK ASSESSMENT REPORTING

Producing a comprehensive security risk assessment (SRA) report highlighting all findings and recommendations can enable senior officials to make well-informed mitigation decisions. Accurate judgments are based on methodical assessments of known factors and on harnessing the collective input

Chart 5 - Countermeasure Assessment Example

(E) Existing / (O) Ordered / (R) Requested (in order of priority)				*Undesirable Event*	Terrorist attacks	Internal & external thefts	Cyber-based attacks	Detection of UC operations	Improper security discipline	Loss power & commo.	Theft of weapons & equip.	Facility penetrations	Inadequate parking	Loss of public trust	Notes
	Countermeasure	***Number & Cost***	***CM Effect***												
E #1	*Provide semi-annual security refresher training to all.*	No extra cost.	*Deter Defend*		*	*	*	*	*		*	*			Conduct March & Sept.
E #2	*Increase operational security into all investigations.*	No extra cost.	*Detect Defeat*		*	*	*	*	*		*			*	Increase ASAP
O #1	*Increase community relations & public affairs projects.*	$ 3,000.	*Deter Detect Defeat*		*									*	Conduct ASAP
O #2	*Purchase secure containers for all removable media.*	22 x $350. = $7,700.	*Deter Deny*		*	*			*			*			Ordered. ETA Sep. 2005
R #1	*Purchase secure radio & phone systems.*	$225,000.	*Deter*				*		*	*					Request ASAP
R #2	*Install securer doors & locks on arms, gear, & evidence rooms.*	10 x $300. = $3,000.	*Deny Delay*		*	*			*	*	*				Request next month
R #3	*Construct detached prisoner processing facility next to HQ.*	$ 92,500.	*Deny Defend*		*	*			*		*	*			Request next year

CM Effect: Deter, Detect, Deny, Delay, Defend, or Defeat.

from subject-matter experts to derive acceptable levels of risk and courses of action.

Based on available and projected resources, decision makers may implement countermeasures in varying intensities or at select locations, or they may accept risk conditions based on existing priorities, resources, and threat status. An SRA report should contain several components.

- Executive summary highlighting the major findings, requests, and suggestions
- Background information defining the purpose of the assessment
- Overview describing ARM to familiarize readers with the process
- Status of any related assessment reports received

from other agencies and substations
- Detailed findings of assessed assets, threats, and vulnerabilities
- Review of calculated security or operational risks
- Countermeasure options, including the types and quantities desired
- Critical concerns and prioritized specific problems
- Detailed recommendations and external support requests
- A security program plan describing the department's plan of action (e.g., goals, objectives, and actions) to mitigate risks
- Discussion of planning, programming, and budgeting requirements
- Overall lessons learned and information for sharing
- Predictive risk analysis discussing future risks and preventive measures
- Summary and conclusion recapping major findings and recommendations

FUTURE CHALLENGES

The character of emerging threats is changing rapidly. Today, law enforcement agencies are challenged by multiple asymmetric perils: domestic violence, criminal enterprises, white-collar crimes, cyber-based offenses, transient agitators, public corruption, and assorted threats of terrorism. Emerging threats include old, reemerging dangers, such as increasing street gang violence and the influence of incarcerated criminals continuing to conduct unlawful enterprises from prisons; the use of assorted improvised explosive devices (IEDs); the increasing menace of weapons of mass destruction potentially involving chemical, biological, radiological, nuclear, and high-explosive devices; new alliances and symbiotic relationships between criminals, terrorists, and foreign governments, in which criminals and foreign intelligence services exchange resources (e.g., weapons, information, money, and hostages) with terrorists; and still-undetected hidden dangers.

> ***"Conventional external threats involve individuals, domestic groups, and sometimes foreign entities."***

Detecting, identifying, and neutralizing threats and adversaries require a holistic approach by assembling separate pieces of the puzzle to see the big picture of the hostile forces (e.g., criminals, extremists, and terrorists). Common profiles of antagonists include a thorough understanding of the following:

- Goals: What specific objectives are the adversaries trying to achieve (e.g., to influence, disrupt, or destroy)?
- Motivation: What stimulates them to do what they do (e.g., for domination, fear, greed, or prestige)?
- History: What are their social, cultural, political, religious, and psychological influences (e.g., based on animosity, vengeance, or ideology)?
- Funding: What are their sources of monetary resources (e.g., foreign sponsors, criminal enterprises, or false fronts)?
- Support structure: What basic framework supports their operations and daily living activities (e.g., lodging, training, transporting, and sustaining)?
- Skills: What are their technical and tactical skills (e.g., weapons, explosives, specialized training, and language)?

- Collection: What are their intelligence collection sources and methods (e.g., insiders, visitors, or open sources)?
- Knowledge: What do they know about their targets (e.g., their assets, vulnerabilities, and countermeasures)?
- Tools: What specific tools do they possess (e.g., identity papers, vehicles, and computers)?
- Weapons: What specific weapons do they have (e.g., small arms, IEDs, or weapons of mass destruction)?
- Opportunities: What opportunities may be or become available to strike (e.g., mass public gatherings, visiting dignitaries, building repairs, or open gaps)?
- Action: What are their action capabilities (e.g., Are they motivated, organized, equipped, trained, supported, knowledgeable, and readied attackers?)?

In assessing emerging threats, law enforcement agencies can target and exploit some of an adversary's common operating methods and techniques. These include increased use of physical, imagery, and technical surveillance to identify the target's vulnerabilities; applied use of long-term meticulous planning and preparation; attempts to control circumstances and timing of when operations will commence; use of multiple independent cells with the same target; simultaneous attacks of soft-target and high-payoff objectives to create mass fear, havoc, and casualties; and increased support networks for funds, recruitment, contacts, safe houses, false identities and cover stories, training, weapons, explosives, intelligence, communications, transportation, and escape plans or death benefits for surviving family members.

First and foremost, mitigation of emerging threats requires the ability to think and

A New Generation of Adversaries

The acronym CAS-DRI-VARS may characterize some fundamental operating methods that free-ranging adversaries exploit throughout the world.

- Creative: applying innovative use of the ancient arts of unconventional warfare
- Asymmetrical: launching multifaceted physical, political, informational, and cyberattacks
- Secretive: cloaking in multiple layers and compartmented cells
- Deceptive: misleading and manipulative in their intent and behavior
- Resourceful: maximizing the use of available resources to achieve their objectives
- Intelligent: capitalizing on detailed planning and orchestration
- Visionary: foreseeing the third and fourth order of effects of their actions
- Adaptable: evolving and adjusting with each new countermeasure
- Ruthless: striking with brute violence against the innocents
- Sophisticated: employing intricate ploys and strategies

act beyond conventional wisdom. That is, risk managers and key decision makers must assess the last attack, but not plan exclusively for the same attack. Law enforcement officials should enhance their abilities to be—

- receptive to both new innovations and old solutions;
- thorough in assessment, planning, and execution;
- resourceful in synergizing use of all assets;
- unpredictable in overt behavior;
- uncompromising in maintaining the highest security and operational standards;
- practical in applying preventive measures; and
- flexible and bold in countering new challenges.

CONCLUSION

Identifying and thoroughly understanding local and regional threats give law enforcement agencies a distinct advantage in better preparing for a wide range of risks and challenges. Today's criminals, extremists, and terrorists continue to practice the ancient principles of lawlessness: striking when and where they are most ready and when they perceive that the law is absent or its enforcers are least prepared. Departments must be able to recognize potential threats and have plans of action to counter a myriad of internal and external risks.

Assessments can provide risk managers and decision makers with a baseline of vital information and collective trends that ultimately impacts strategic planning efforts.

> ***"Assessing threats involves identifying and assessing all of the threats associated with each asset."***

Reports give focus for future security and operational initiatives via the opportunity to realign priorities, update monetary funding, and share lessons learned with the public safety community.

Law enforcement agencies should perform risk assessments annually and whenever a major adverse incident occurs, key leadership changes, operations relocate, and physical or procedural security modifications transpire. Analytical risk management (ARM) assessments and accompanying security risk assessment (SRA) reports support planners and managers in developing comprehensive security programs to mitigate risks, justify budget and resource requests, and identify ways to improve security departmentwide.

ARM assessments and SRA reports are a snapshot of current assets, threats, vulnerabilities, and risks. ARM offers a flexible method for examining security and operational readiness and for developing cost-effective countermeasure options, whereas SRA reports provide a formal audit trail leading to well-informed decision making. Together, these tools can help the law enforcement community enhance its ability to face the rigors of tomorrow's world of uncertainty. ✦

Endnotes

[1] The FBI recently completed an assessment to evaluate its own security posture using ARM, which the U.S. Security Policy Board's Risk Management Training Group developed. The FBI's version of ARM involves a six-step process that identifies an organization's assets, threats, vulnerabilities, risks, and needed countermeasures and then develops a security risk assessment (SRA) report.

Please forward questions, comments, and suggestions to deanlee@leo.gov or phone Dr. Lee at 202-324-3173.
The FBI's Security Division fully supports the dedicated law enforcement professionals serving communities throughout the United States and the free world.

Early Detection of the Problem Officer

By Dino DeCrescenzo

Sadly, a disturbing trend has begun to emerge concerning the law enforcement profession. That is, allegations against those officers facing suspension or termination rarely seem to surprise members of their departments and, at times, many residents of their communities. Over the past several decades, investigative journalists have found that in some agencies, as few as 2 percent of officers held responsibility for 50 percent of citizen complaints.[1] In addition, numerous police chiefs reported that 10 percent of their sworn personnel caused 90 percent of the problems.[2] Also, studies on the issue repeatedly indicated that an extremely small and disproportionate number of officers incurred most of the accusations.[3]


© Mark C. Ide

In reality, the majority of law enforcement officers are supremely dedicated individuals severely offended by the behavior and acts committed by those few who have tarnished the image of their profession.[4] These officers and the citizens they serve have begun to demand reasons for why such employees have remained on the job, even though they have violated departmental and societal rules. The awareness of these problem officers has existed for some time. In 1981, the U.S. Commission on Civil Rights recommended that all police departments create an early warning system to identify problem employees who often receive the highest number of complaints or display patterns of inappropriate behavior.[5] In today's world of terrorists and increasingly violent criminals, such efforts may prove more important than ever before.

Intervention Approach

According to the U.S. Department of Justice, early warning systems take the form of databases that contain personnel information designed to identify problem behavior and allow early intervention to correct the misconduct. Generally nonpunitive, the systems include peer review, additional training, and counseling. They can provide supervisors and managers with information relating to potential patterns of at-risk conduct. Most systems require intervention after recording a certain number of complaints of a particular type within a specified time frame.[6] Although a few departments use only citizen complaints to select officers for intervention, most rely on a combination of behavior indicators.[7] Early warning systems should consider the totality of officer work histories, including accidents, pursuits, transfers, training, grievances, education, drug usage, civil suits, truthfulness, property damage, discourtesy, false arrest claims, and insubordination.[8] They should track all complaints, sick time used, resisting arrest incidents, assaults on officers, obstruction of officer arrests, and disorderly conduct arrests made by officers.[9] These last four behavior indicators appear to be significant measuring devices of potential problem employees. A higher number of these types of arrests when compared with those of other officers may reveal personnel acting beyond their scope of authority.

The theory behind an early warning system is that such incidents *individually* may mean nothing, but the combined totality of behaviors may signal a developing problem that needs attention.[10] These indicators, compiled into a single place, can flag a potential pattern of problematic behavior and identify an officer at risk of engaging in misconduct.

The phenomenon of early detection or early warning systems within law enforcement agencies is a fairly new concept that has begun to spread more rapidly since Congress passed the Violent Crime Control and Law Enforcement Act, which empowered the federal government to investigate and bring suit against those officers who routinely abused their authority.[11] For the most part, when departments have suits brought against them, they enter into a consent decree with the government agency agreeing on the changes required and to being monitored until the judge lifts the decree.[12] More often than not, the recommendations stemming from such investigations include implementation of an early warning or detection system as a first step in the process of abolishing the pattern and practice of conduct by the officers.

> "Generally nonpunitive, the systems include peer review, additional training, and counseling."

Research Findings

The first in-depth study of early warning systems found that 27 percent of the agencies surveyed in 1999 had such a mechanism in place while another 12 percent planned on implementing one.[13] The participating agencies were police departments employing a minimum of 80 officers and serving populations of at least 50,000. However, 87 percent of police departments in the United States have fewer than 25 sworn officers.[14] So, while less than 40 percent of the large agencies surveyed either had or planned to have an early warning system in 1999, the majority of police departments in the country most likely did not have nor plan on implementing such a system at the time.

If administered properly, an early warning and detection system should allow the department to quickly intervene and help modify the behavior of the officers identified. Moreover, a successful early detection system not only can identify negative behavior but also can recognize conduct worthy of commendation.[15] The study further indicated that early warning systems substantially reduced citizen complaints and other problematic behavior. For example, three large police departments with early warning systems in effect for at least 4 years had substantially fewer citizen complaints and use-of-force incidents after the intervention. A successful system can benefit the entire agency, the community, and the troubled or problem officer with prompt intervention administered properly. Experts stress that using an early warning system to punish officers will undermine its effectiveness, but applying the information learned from the data to counsel and train them will expand its value.[16]

Some departments have successfully employed early warning systems for over a decade with beneficial results.[17] However, these programs still may not accurately identify every specific pattern of behavior that may ultimately lead to misconduct. In addition, the study found that no standards had been established for identifying officers in the early warning systems examined. Instead, only a general agreement existed on some of the criteria that should influence their selection.[18] These issues demonstrate that agencies must carefully analyze the information compiled on their personnel and establish strict selection guidelines to ensure that they correctly determine those officers in need of intervention.

Finally, the study noted that the implementation of an early warning system can prove compatible with both problem-oriented and community policing. The law enforcement administrator can incorporate the warning system into the department's overall philosophy and goals,

recognizing that the new system must involve counseling and training as the main objective in modifying the behaviors of the officers selected and flagged for intervention. The administrator, however, must remember that the police union and the officers may suspect a new warning system and possibly resist its implementation. One early warning discipline system stressed the police union's involvement in the process prior to implementation of a program that provided predictable sanctions agreed upon by management and the union.[19] Because most complaints by unions involve the unequal treatment of personnel and ambiguous, unknown, or unpredictable punishments, this system established a disciplinary matrix with minimum and maximum penalties and ensured that the administration and the collective bargaining unit agreed upon predictable, reliable, equitable, and valid sanctions. Such involvement by the union or collective bargaining unit can greatly increase the success of an early warning system.

> "Some departments have successfully employed early warning systems for over a decade with beneficial results."

Positive Change

Law enforcement agencies throughout this country generally have pursued a traditional approach when dealing with officer misconduct.[20] Most have dealt with this issue through reactive as opposed to proactive efforts, primarily using citizen and internal complaints to identify such behavior. In addition, most departments impose corrective action only after the misconduct has occurred.

To effect positive change in the behavior of the few officers that create the majority of problems, departments must begin to take sufficient action against those repeatedly accused of excessive force and continually look for patterns in officer conduct.[21] They also must seriously discipline such personnel, not merely reassign them to other duties. Finally, agencies must provide troubled officers with counseling and other services. As one official said, "We have a tendency to go from zero to 60, by focusing only on the egregious, but not having a system to correct or discipline the behavior that is nonegregious."[22]

Officers who have exhibited less than stellar behavior need help to return to their former standards of professionalism. Departments should endeavor to find out what these officers need to overcome their problems and, once again, become valuable, contributing members of their profession. To this end, an early warning system can offer an effective approach for agencies to use.

Conclusion

Today's law enforcement administrators must identify problem officers and intervene appropriately with counseling, training, and other methods in an attempt to modify and change their behavior. Managers will benefit their departments, communities, and problem officers with the implementation of a properly administered early warning system. Such an approach can help agencies combat the disturbing trend that seems to indicate that they disregard officer misconduct.

Early warning systems demonstrate that departments and administrators have developed a clear policy regarding misconduct, have put a program in place to correct negative behavior, and have made a good-faith effort to identify employees whose performance is less than satisfactory.[23] The majority of their officers who valiantly place themselves in harm's way every day to protect the citizens of their communities deserve no less. ✦

Endnotes

[1] C.R. Swanson, L. Territo, and R.W. Taylor, *Police Administration: Structures, Processes, and Behavior*, 6th ed. (Upper Saddle River, NJ: Prentice Hall, 2004).

[2] S. Walker, G.P. Alpert, and D.J. Kenney, "Early Warning Systems: Responding to the Problem Police Officer," *National Institute of Justice Journal* (July 2001); retrieved on January 28, 2005, from *http://www.ncjrs.org/pdffiles1/nij/188565.pdf*.

[3] S. Slahor, "Earlier Is Better When Solving Problems," *Law and Order*, June 2004, 6.

[4] J. Arnold, "Special Report II: Ethics—Early Misconduct Detection," *Law and Order*, August 2001, 8.

[5] Supra note 2.

[6] Supra note 4.

[7] Supra note 2.

[8] Supra note 3.

[9] T.F. Kennedy, *Preventing, Detecting, and Investigating Employee Misconduct*, paper presented at a Roger Williams University Conference, Bristol, RI, October 2003.

[10] R.G. Dunlop and J. Adams, "System to Spot Troubled Officers Not Fully Used: Goal Is to Detect Small Problems, Prevent Big Ones," *Louisville Courier Journal*, April 2, 2000.

[11] "Pittsburgh's Experience with Police Monitoring," *Vera Institute of Justice*, June 17, 2004; retrieved on January 28, 2005, from *http://www.vera.org/project/project1_1.asp?section_id=7&project_id=13*.

[12] Ibid.

[13] Supra note 2.

[14] S.F. Kelly, "Internal Affairs: Issues for Small Police Departments," *FBI Law Enforcement Bulletin*, July 2003, 1-6.

[15] Supra note 3.

[16] "Best Early Warning Tool Is Informative," *Organized Crime Digest* 22, no. 13 (August 10, 2001).

[17] Supra note 4.

[18] Supra note 2.

[19] R.W. Serpas, J.W. Olson, and B.D. Jones, "An Employee Disciplinary System That Makes Sense," *The Police Chief*, September 2003.

[20] Supra note 4.

[21] D. Washburn, D. Hasemyer, and M. Arner, "A Question of Force: Dealing with Multiple Shooters Has Been a 'Huge' Issue," *The San Diego Union-Tribune*, January 19, 2003; retrieved from *http://www.signonsandiego.comnews/reports/shootings/20030122-9999_mz1n19questn.htm*.

[22] Supra note 3.

[23] Supra note 2.

Detective Sergeant DeCrescenzo serves with the Barrington, Rhode Island, Police Department.

Wanted: Photographs

The *Bulletin* staff is always on the lookout for dynamic, law enforcement-related photos for possible publication in the magazine. We are interested in photos that visually depict the many aspects of the law enforcement profession and illustrate the various tasks law enforcement personnel perform.

We can use either black-and-white glossy or color prints or slides, although we prefer prints (5x7 or 8x10). We will give appropriate credit to photographers when their work appears in the magazine. Contributors should send duplicate, not original, prints as we do not accept responsibility for damaged or lost prints. Send photographs to:

Art Director
FBI Law Enforcement Bulletin, FBI Academy,
Madison Building,
Room 201, Quantico,
VA 22135.

ViCAP Alert

Robert Mark Edwards

DOBs Edwards used: 6/14/61, 6/15/60, 6/14/58, 6/15/61

Edwards' FBI number: 41518W11

SSANs Edwards used:

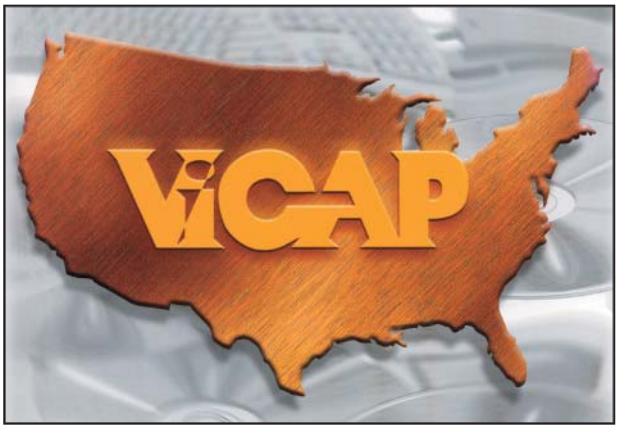
552-43-8728, 553-47-2874

Edwards' physical description:

Height: 5'8" Weight: 150 lbs.

Hair: Brown Eyes: Blue

Aliases Edwards used: Kirk Edward Bell, Paul Robert Smith, Mark Edward Robert, Mark R. Edwards, Bobby Edwards, Jim Portillo, James Mark Portillo, Rob Edwards



Any agency that believes Edwards' modus operandi might match their cold cases should contact SSA Jim McNamara, Federal Bureau of Investigation, Critical Incident Response Group, Behavioral Analysis Unit-2, at 703-632-4325 for additional information.

Currently incarcerated in California on a first-degree murder conviction, Robert Mark Edwards also was convicted of second-degree murder and five other felony counts in Hawaii. Law enforcement authorities believe he may have committed other homicides, attempted homicides, or violent sexual assaults.

Crime Scenes

In May 1986, Edwards murdered 55-year-old realtor Marjorie Deeble in her apartment in Los Alamitos, California. Marjorie had been beaten about the head, and her nose was broken. She was found in a nightgown on the floor with her hands tied behind her back with part of her nightgown and a telephone cord. Her head, neck, and shoulders were suspended about 6 inches off the floor by a noose formed by a belt and tied to the top drawer of a chest. Marks on her ankles indicated she may have had her legs tied at one time, and adhesive tape residue was found on her cheeks, suggesting a gag. Both of Marjorie's eardrums were lacerated or torn. She had been sexually assaulted vaginally with a mousse can at some point. Some items of jewelry were missing from her residence. Edwards was dating Marjorie's daughter at the time.

In January 1993, 67-year-old Muriel Delbecq, a realtor who lived in Alaska but spent 2 to 3 months each year in Hawaii, was found murdered in her apartment in Kihei, Maui. She had been strangled and beaten about the head and face. Her pubic hair appeared to have been shaved or cut, and there were contusions and abrasions on her breasts. Muriel had been sexually assaulted vaginally with a hair spray can with such force that it penetrated her abdominal cavity. The insertion occurred ante- or perimortem. Muriel's wedding ring and purse were taken. Numerous items from the victim's house, including panties and bras, were found in a trash bin across the street from the murder site. One of the bras was cut between the cups and the tips of the cups had been removed, and one pair of panties was cut open. Edwards lived within a block of Muriel's residence.

Modus Operandi

Both of Edwards' known victims have been older white females who were low- to moderate-risk victims living alone in ground-floor apartments. It appears they were sleeping or preparing to go to bed when attacked, apparently by a surprise assault. Ante- or perimortem foreign object insertion, both vaginally and anally, was present in both cases, although a lack of penile-vaginal penetration existed.

A former girlfriend reported that Edwards liked to tie her up during sex and at least twice attempted to sodomize her with a bottle. She said he would follow her and park near her place of employment, and he threatened to kill her if she discontinued their relationship.

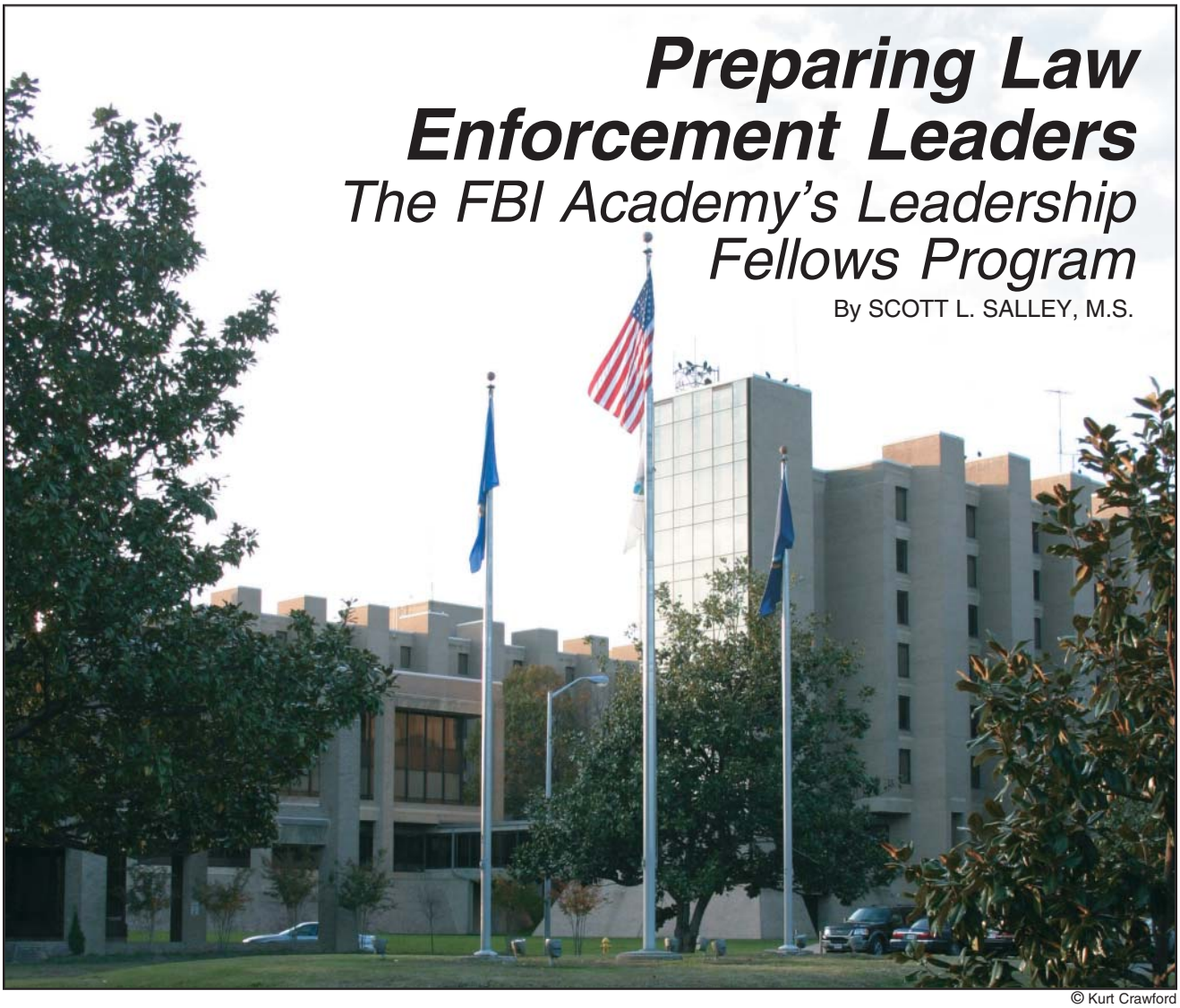
Alert to Law Enforcement

Edwards has an extensive criminal history in California, including such charges as burglary, grand theft auto, drunk driving, possession of a controlled substance, trespassing, peeping, and receiving stolen property. He was in custody in California from July 1984 to December 1985, from December 1988 to November 1989, and was arrested for the murder of Muriel Delbecq in Hawaii on February 2, 1993. He has been in custody since that time. ✦

Preparing Law Enforcement Leaders

The FBI Academy's Leadership Fellows Program

By SCOTT L. SALLEY, M.S.



© Kurt Crawford

How do law enforcement agencies prepare their command staff members for the challenges that will confront them as they assume additional responsibilities? While no magic formula exists, there is a method to expedite the problem-solving experience that will help mold these individuals into successful leaders. To this end, chiefs, sheriffs, and senior agents should consider the FBI Academy's Leadership Fellows Program located in Quantico, Virginia.

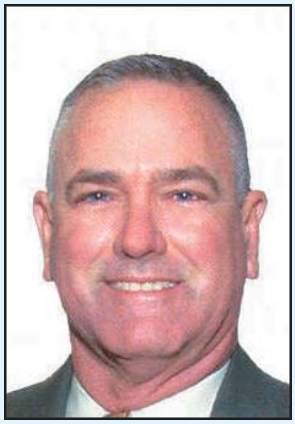
Program Overview

Started in 2000 and supervised by the Leadership Development Institute (LDI),[1] this 1-year program serves to enhance the leadership skills of individuals in command-level positions and broaden their exposure to both the domestic and international law enforcement communities. Fellows spend 6 months at the academy and the remaining 6 at their respective agencies or at Quantico for additional research and study.

What separates this program from others that emphasize leadership development? First of all, participants find that living at the academy while interacting with the staff, FBI

National Academy (NA) students, and new agent trainees and experiencing a wide selection of training with law enforcement members from around the world provide tremendous value. Additionally, the close proximity to Washington, D.C., offers access to an enormous selection of resources, including museums, federal law enforcement agencies, historic sites, government institutions, and seemingly endless educational opportunities.

> ***"As departments seek to prepare leaders in their ranks, they realize that no easy method exists. However, this program offers a proven method...."***



Captain Salley serves with the Collier County, Florida, Sheriff's Office.

Also important is the program's "trilogy"; participants complete these three components at the end of the fellowship. One, the individual works on projects for the FBI, such as instructing certain classes, organizing training sessions, assisting academy staff with a variety of tasks, and teaching overseas at the International Law Enforcement Academy (ILEA) in Budapest, Hungary.

Two, the participant conducts a research project for the sponsoring agency that brings immediate value to the training. For the assignment, the department head identifies a need for the agency; in addressing this, the fellow has some of the best resources in the world available. The department, the FBI, and the individual all derive substantial benefit from this study.

Three, the participant follows a personal development path, or a list of goals with anticipated outcomes. These could include earning a "yellow brick"[2] for physical improvement with the FBI NA, reading a certain number of books pertaining to management topics, learning new computer skills, devising a personal or agency wellness plan, or attending leadership development training, such as the Law Enforcement Executive Development Seminar (LEEDS).

Application Process

Interested officers must understand the time and dedication the fellowship demands. The program involves a partnership between the applicant, immediate family members, the head of the sponsoring agency, and the FBI Academy. Sometimes, this also includes friends, other relatives, and the community where the fellow resides. Support from all affected parties is needed, and a signed statement by the department head constitutes one of the requirements for admission. While making this important decision, individuals can gain additional information about the program and its advantages by contacting the FBI Academy and talking with any of the current fellows or obtaining a list of alumni and communicating with former participants.

For consideration, prospective fellows submit a completed application[3] to LDI. Each becomes rated on a point system based on several factors, such as law enforcement experience, community involvement, education, and position. Also required as part of the package is supporting documentation, such as newspaper articles and transcripts—the more the applicant includes, the better the chances for acceptance. Organization and clarity help

ensure an effective overall presentation.

Prospects can call the program manager regarding status for approximately 30 days after submission of an application. Upon acceptance, individuals will receive a formal letter from the FBI; the agency head also will get a copy. Then, the tasks of scheduling and preparing for this 1-year journey begin.

Outcome Achieved

Fellows will share many of the same experiences and educational benefits, but each also will take away something different. Largely, this is determined by individual choice. For example, one participant may travel to Europe to instruct at ILEA, while another may assist with a presentation at one of the regional command colleges in the United States. Fellows will find a lot of flexibility for optimizing their involvement in the program.

How does participation in the fellowship benefit the sponsoring agency? Its command-level personnel enjoy enrichment through the interaction with the course material, instructors, and students; strengthening of their organizational skills; enhanced networking, through which they gain valuable relationships that will aid them upon their return to duty; and improved confidence, experience, and professionalism.

Also, the program can help department heads prepare for the future. In this regard, chiefs can use it to ensure that command staff members have the necessary tools for maintaining or improving the current status of law enforcement in the communities they serve. The fellowship has graduated individuals that live in areas located across the United States and abroad, and the concentrated studies and hands-on involvement by participants have been observed as a significant benefit to agencies both large and small.

Expectations of Fellows

Fellows, either independently or in cooperation with other participants and FBI Academy faculty, must—

- teach and attend classes;
- conduct research;
- manage projects;
- facilitate meetings;
- coordinate programs;
- attend professional conferences;
- write publishable articles or documents; and
- establish professional networks.

Conclusion

Law enforcement agencies continually face new challenges in an ever-changing world. Department leaders need preparation to address them. To this end, the FBI Academy's Leadership Fellows Program can help. For example, as one fellow stated, "Law enforcement has changed radically since September 11, 2001, and having a command staff member familiar with the FBI Academy and the associated services that the FBI provides has been an important link for obtaining information regarding domestic and international terrorism."

As departments seek to prepare leaders in their ranks, they realize that no easy method exists. However, this program offers a proven method for accomplishing this goal and represents an important

Requirements for Admission

The FBI awards 5 to 10 fellowships each year to candidates who must—

- be sworn officers serving in a command staff position;
- hold a bachelor's degree (advanced degree preferred);
- come highly recommended by their agency's chief executive; and
- be available to serve as a fellow for 12 months, with at least 6 continuous months spent in residence at the academy.

consideration for agencies in this country and abroad. ✦

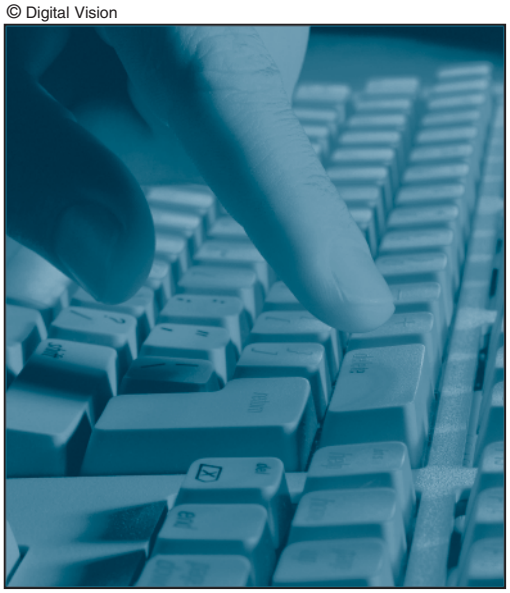
Endnotes

[1] LDI strives to enhance effective, practical, and creative leadership and management practices and encourage a spirit of cooperation among FBI, municipal, county, state, and international law enforcement leaders through the design and administration of programs and developmental experiences that foster growth and lifelong learning. For additional information on the unit, as well as the programs mentioned throughout this article, visit *http://www.fbi.gov*.

[2] See Patti Ebling, "Physical Fitness in Law Enforcement: Follow the Yellow Brick Road," *FBI Law Enforcement Bulletin*, October 2002, 1-5.

[3] Candidates may obtain an application from the Leadership Development Institute, Attn: Leadership Fellows Program, FBI Academy, Quantico, VA 22135.

The *Bulletin's* E-mail Address



The *FBI Law Enforcement Bulletin* staff invites you to communicate with us via e-mail. Our Internet address is *leb@fbiacademy.edu*.

We would like to know your thoughts on contemporary law enforcement issues. We welcome your comments, questions, and suggestions about the magazine. Please include your name, title, and agency on all e-mail messages.

Also, the *Bulletin* is available for viewing or downloading on a number of computer services, as well as the FBI's home page. The home page address is *http://www.fbi.gov*.

Bulletin Reports

Victims

Crimes Against Persons Age 65 or Older, 1993-2002 presents data from the National Crime Victimization Survey and the Uniform Crime Reports comparing incidents targeting persons 65 years of age or older with those involving younger age groups. Crime rates are presented for murder, rape/sexual assault, robbery, aggravated and simple assault, purse snatching/pocket picking, household burglary, and motor vehicle theft and property theft. The report describes trends in violent and property crimes between 1993 and 2002 and discusses characteristics of the incidents, including injury to victims, self-protective measures used, whether weapons were present, time and place of occurrences, and victim-offender relationships. Crimes include both reported and nonreported. This publication is available online at *http://www.ojp.usdoj.gov/bjs/abstract/cpa6502.htm* or by contacting the National Criminal Justice Reference Service at 800-851-3420.

Human Trafficking

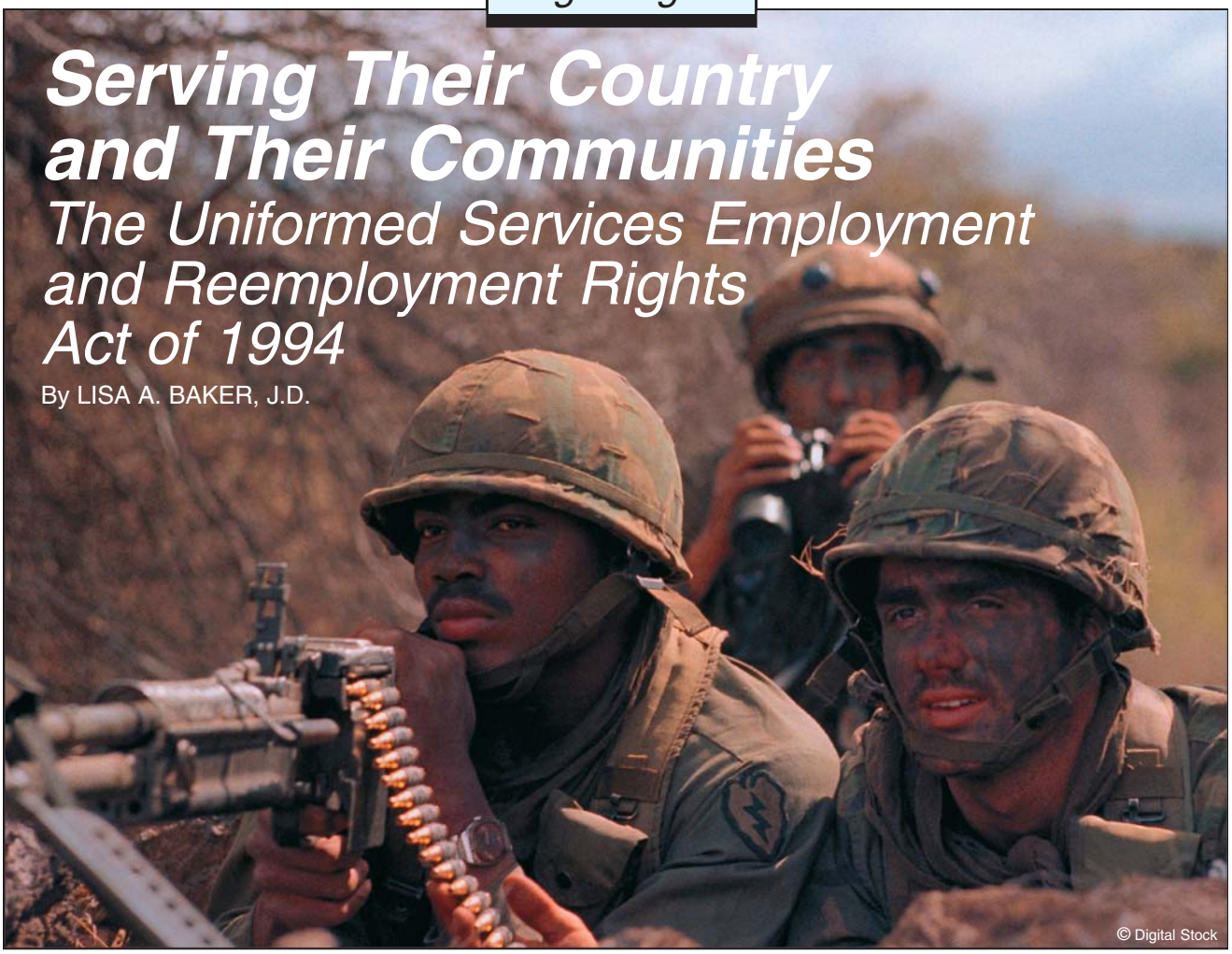
The National Institute of Justice (NIJ) offers *Characteristics of Chinese Human Smugglers*, which presents findings of a study that uncovered the inner workings of Chinese human smuggling organizations by going right to the source—the smugglers themselves. Researchers found that most of these individuals are ordinary citizens whose social networks provide the necessary connections and resources to profit from human trade. Enforcement efforts require consideration of the unique organization of smuggling enterprises and how smugglers are perceived by themselves and their clients. This report is available electronically at *http://www.ncjrs.org/pdffiles1/nij/204989.pdf* or by calling the National Criminal Justice Reference Service at 800-851-3420.

Bulletin Reports is an edited collection of criminal justice studies, reports, and project findings. Send your material for consideration to: *FBI Law Enforcement Bulletin*, Room 201, Madison Building, FBI Academy, Quantico, VA 22135. (NOTE: The material in this section is intended to be strictly an information source and should not be considered an endorsement by the FBI for any product or service.)

Serving Their Country and Their Communities

The Uniformed Services Employment and Reemployment Rights Act of 1994

By LISA A. BAKER, J.D.



Hundreds of thousands of "citizen soldiers" have been called to active duty in the military since the events of September 11, 2001. These citizen soldiers leave their families and jobs behind, often leaving with questions about their future employment security when they return, as well as benefits, such as health insurance and their pensions, while they are away.[1] In addition, many employers find themselves wondering what responsibilities they owe the departing employees during their absence and upon return to civilian life. Not surprisingly, the law enforcement community presently is dealing quite often with these issues given the significant representation of prior military in law enforcement. Given the impact continued military service can have on the personal and professional lives of law enforcement personnel, it is important that both law enforcement employers and employees who leave to perform military duty have an understanding of the rights and obligations under the Uniformed Services Employment and Reemployment Rights Act of 1994 (USERRA).[2]

This article provides a general overview of the background and purpose behind USERRA in addition to the rights and obligations of the employee and employer and the prohibition against discrimination based on active duty. Issues

addressed include the right to reemployment, the impact active duty has on benefits, such as health insurance and pensions, and notice requirements imposed on both employers and employees. The article is intended only as a general overview of key aspects of USERRA. For more specific information, the reader may want to refer to the U.S. Department of Labor (DOL) at *http://www.dol.gov*. In this Web site, the DOL's Veterans' Employment and Training Services (VETS) has published extensive information regarding USERRA, including proposed regulations interpreting USERRA, published on September 20, 2004.[3]

BACKGROUND AND SCOPE

USERRA was enacted by Congress in 1994 for the purpose of prohibiting discrimination against individuals because of their voluntary or involuntary military service and encouraging military service by lessening the disadvantages associated with such service when a civilian career is impacted.[4] USERRA has broad application, covering nearly all employees, including part-time and probationary employees, as well as all U.S. employers, whether in the private or public sector and regardless of size.[5] The term "employer" also includes individuals.[6] This has been interpreted as allowing an individual seeking enforcement of USERRA to pursue an action not just against the employing entity but also against *individuals* who have authority within the employing entity regarding the employment decision.[7]

Congress also provided a comprehensive definition of "uniformed services." This is defined to include employees who serve in the Army, Navy, Air Force, Marine Corps, Coast Guard, as well as all Reserve components of each, the Army or Air National Guard, and the Commissioned Corps of the Public Health Service. In addition, the president has the authority to identify any other category of persons as covered by USERRA during time of war or emergency.

Congress also clarified the type of "uniform service" which triggers the rights and responsibilities provided for in USERRA.[8] Included within the covered service is duty performed, regardless of whether it is voluntary or involuntary, while in active duty, active duty for training, as well as inactive duty training, and full-time National Guard duty. In addition, an employee's absence from work to assess the employee's fitness to take part in any of the above activities also is covered by USERRA. In 2002, Congress expanded USERRA's reach to include public service performed in a crisis situation by including within the definition of "uniform service" duty performed by intermittent disaster personnel for the Public Health Service, as well as time for taking part in training for such activities. Funeral honor duty performed by National

"USERRA was enacted…for the purpose of prohibiting discrimination against individuals because of their voluntary or involuntary military service…."

Special Agent Baker is chief of the Legal Instruction Unit at the FBI Academy.

Guard or reserve members also is included.

In addition, to be eligible for reemployment, the uniform service must be under the authority of the military. In other words, the absences must be connected to actual military service. For example, in *Leisek v. Brightwood Corp.*,[9] John Leisek, a former employee of a company and a member of the National Guard, sued after he was denied reemployment following his absence to participate in National Guard activities. The Court concluded that he had no right to be reemployed as he was not engaged in "uniformed service" at the time of his absence from his employer. Prior to his absence for the guard, Leisek indicated that he would be engaged in Guard duties at various locations and various dates and asked for time off accordingly. He eventually did receive military orders for some of the dates and locations, but not for all of them. The Court held that he was not serving in the "uniformed services" as to those dates for which he was not under orders to serve.

While USERRA applies to all employers, the units comprising the Ready Reserve[10] by statute must be screened to ensure that there are not large numbers of members with "critical civilian skills," and that there are no members who, if mobilized, would "...result in extreme…community hardship."[11]

PROHIBITION ON DISCRIMINATION

USERRA contains an antidiscrimination provision designed to protect those who have served, as well as those who remain in the military in some capacity, from discrimination. The prohibition against discrimination protects not only on-board employees but applicants for employers as well. An employer is prohibited from denying any person initial employment, reemployment, retention in employment, promotion or any benefit of employment based on an individual's membership or application for membership and the activities associated therewith, in the uniformed services.[12] The statute also prohibits retaliation against an individual for seeking enforcement of any right secured under USERRA.[13]

> ***"Employer discrimination is established by showing...military-based activity...was a "motivating factor...."***

Employer discrimination is established by showing the applicant or employee's military-based activity, whether in the form of an application for membership, performance of service or some obligation of service, was a "*motivating factor*" in the employer's decision as opposed to the *sole* factor.[14] The roadmap for a lawsuit under USERRA calls for the initial burden to be on the plaintiff, who must provide sufficient information to support an allegation of discrimination or retaliation on the basis of military service.[15] The employer then may demonstrate that it would have taken the action anyway, without regard to anything protected by USERRA. If the employer successfully demonstrates this nonprohibited reason for the employment action, the plaintiff must then establish that the reason offered really is pretextual and the employment action actually was based on military service. This same litigation roadmap is set forth in USERRA for litigating claims of retaliation.[16]

ELIGIBILITY FOR REEMPLOYMENT

USERRA extends reemployment rights to most employees[17] who have been absent from their positions because of "service in the uniformed services." To be eligible for reemployment, the service

member must meet the following basic requirements:

- notice must have been given to the employer of service in the uniformed services;
- cumulative period of service must not have exceeded 5 years, unless an exception to the 5-year rule applies;
- departure from the uniformed services was not dishonorable or under other punitive conditions; and
- the requestor must have submitted a timely request for reemployment and reported back to their civilian employer in a timely manner.

USERRA does not require the employer to return employees to the exact same position that they occupied before leaving for military service. The manner that the employer places the employees back into the workforce is structured according to the amount of time the employees were on military leave. If the employees were absent for 1 to 90 days, they must be promptly reemployed in the position that they would have occupied had they remained in continuous employment, provided they are qualified for that position or can become qualified after a relatively short training period.[18] If the employees are not qualified for that position, then the employees must be placed in a position closest to the position described above for which the employees are able to perform.[19] In other words, the deployed reservist employees progress as if they had remained in continuous employment.

For employees on military leave for 91 days or more, USERRA provides a hierarchy for the employer to follow. The employer must first consider placement in the job the employees would have held had they remained continuously employed, provided the employees are qualified for a position of like seniority and pay, or if not qualified for such a position, in the position the employees occupied before deployment or one of like seniority and pay.[20] If the employees are not qualified to perform any of the above positions, then the employer must place the employees in another position of lesser status and pay, but it must be closest to the above-described positions as possible.[21] The employer also must provide reasonable opportunities for training to qualify for the higher positions unless to do so would pose an undue hardship to the employer.[22]

> ***USERRA provides for enhanced protections for disabled veterans.***

Time Limits on Service

To qualify for reemployment, the cumulative service generally cannot exceed 5 years. However, exceptions to this 5-year prohibition exist. These exceptions include:

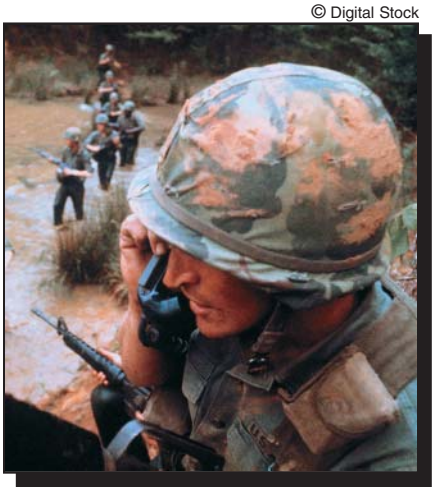
- situations in which the service member cannot obtain a release through no fault of their own;
- involuntary service during a domestic emergency or national security crisis;
- service pursuant to an order to remain on active duty because of war or national emergency;
- active duty by volunteers supporting "operational missions" for which members of the Select Reserve have been ordered to active duty without their consent;
- service by volunteers in support of a "critical mission";
- federal service by members of the National Guard called into service to suppress insurrection; and
- service connected to training.[23]

USERRA and Disabled Veterans

USERRA provides for enhanced protections for disabled veterans. When seeking reemployment, employers are required to undertake reasonable efforts to accommodate their disabilities so they can be placed in a position they would have occupied had they remained in continuous employment.[24] If an employee, despite the efforts to provide training, is unable to perform the functions required of that position, then the employer must place the employee in a position of equivalent seniority, status and pay, provided the employee is qualified to perform that job. If that fails, then the employee must be placed in a position as close to the above as the employee may be able to perform.[25]

Time Limits for Reporting Back to Civilian Employment

Once the deployment ends, USERRA provides a timetable for employees to report back to work.[26] If the service was less than 30 days or for purposes of taking a fitness exam, the employees must report back to work no later than the first regularly scheduled workday that would fall 8 hours after the end of the calendar day. This may be delayed if circumstances arise out of the control of the employees. If the service is for 31 days up to 180 days, the employees must submit an application for reemployment no later than 14 days after completion of service. For service beyond 180 days, the application must be submitted no more than 90 days after the end of service. For employees injured or disabled as a result of their service, the reporting deadline may be extended.[27]



USERRA AND SALARY, HEALTH BENEFITS AND PENSION

No Requirement to Provide Paid Leave

USERRA does not require employers to pay employees wages during any period of military leave. An employer, of course, may choose to do so, or may opt to pay, for example, the difference between the military pay and the employee's regular salary.

Health Benefits

A common concern for reservists activated and deployed is the impact their absence from their civilian job will have on employer-provided health benefits. Generally, if the period of leave is 30 days or less, the employer's health insurance benefits remain intact. If the leave is for more than 30 days, employees and their dependants should be covered by military-provided health care benefits. In addition, other federal provisions offer reservists protection by enabling them to continue their health care insurance. The Consolidated Omnibus Budget Reconciliation Act (COBRA) and USERRA allow for health care coverage rights to employees after an event in employment such as a reduction in hours worked due to military deployment. This extended coverage is good for a period of up to 18 months.

In addition, the Health Insurance Portability and Accountability Act (HIPPA) also recognizes the ability of some individuals to enroll in another health insurance plan if one is available. For example, spouses may have a health insurance plan available through their employer that they may wish to take advantage of during the time of deployment. HIPPA allows for access to this plan regardless of the existence of set enrollment periods.[28]

Pensions and other Employer Benefits

When in leave status for military service, employees are to be viewed as though they are continuously employed for purposes of seniority and pension benefits.[29] In addition, employees exercising their rights under USERRA are entitled to the same benefits as those generally provided to other employees on unpaid leave.

USERRA and the Family Medical Leave Act

The Family Medical Leave Act (FMLA) provides for 12 workweeks of unpaid leave to address a serious health condition of an employee or a family member or to take time off to care for a newborn or adoptee. To be eligible, employees must have worked for the employer for a minium of 12 months and at least 1,250 hours for that employer.[30] Questions regarding the right to use FMLA leave shortly after returning to the workforce from active duty have arisen in light of the requirements regarding employment for the employer preceding the request for FMLA leave. In a DOL Memorandum dated July 22, 2002, available on the DOL Web site at *http://www.dol.gov/vets*, the DOL advised that individuals reemployed following military duty are entitled to the rights and benefits they would have earned if they had remained in civilian employment. The time spent serving in the military is to be counted for FMLA purposes as if the employees never broke service.

NOTICE UNDER USERRA

USERRA requires employees to provide notice to their employers of their intent to take military leave, unless to do so is not feasible or precluded by military necessity.[31] The employer may require written documentation regarding the military leave if it is for more than 30 days.[32]

> ***Generally, if the period of leave is 30 days or less, the employer's health insurance benefits remain intact.***

In 2004, Congress passed the Veterans Benefits Improvement Act (VBIA), which amended USERRA by adding a requirement that employers provide notice of the rights, privileges, and obligations of employees and employers under USERRA.[33] On March 10, 2005, the DOL published an interim final rule, setting forth language to be used by employers to comply with the notice requirement.[34] Generally, the notice includes a description of the reemployment rights of those who voluntarily or involuntarily leave employment for military service, as well as the prohibition against discrimination on the basis of military service and the right to be free from retaliation for seeking enforcement of USERRA. The notice also contains a brief summary on the health benefits attendant to military deployment and a description of the enforcement mechanism.[35]

ENFORCEMENT AND REMEDIES

The statute offers different avenues for an individual to pursue relief. Administrative recourse may be sought through VETS within the Department of Labor. VETS offers guidance on the interpretation and application of USERRA and will investigate complaints, although a complainant has the option of pursing administrative recourse.[36] A complainant also has the ability to request that the U.S. attorney general consider their complaint. If determined to be meritorious, the attorney general may pursue the case for the complainant. Individuals also have the right to pursue the matter in civil court themselves if they choose not to file with VETS or if the attorney

general refuses to pursue the matter.

USERRA allows for the awarding of double dam-ages (double the amount of wages and back pay) if the employer's actions in violating USERRA are "willful." In addition to wage-related damages, the court also may grant attorney fees, expert witness fees, and other similar types of expenses.

CONCLUSION

Recognizing the significant role our citizen soldiers have in protecting this country, Congress has acted to provide job security in their civilian life so that they do not have to choose between serving their country and serving their community. While a civilian employer may face challenges upon the deployment of employees who serve in the reserves, Congress has favored protecting job security upon deployment while attempting to do so in a fair manner to the employer. When assessing the rights and obligations of reservists, employers also should be aware of state laws that may offer even more protections to reservists within that state. ✦

Endnotes

[1] The Department of Labor recently indicated that over 460,000 members of the National Guard and Reserve have been mobilized since September 11, 2001. *See* 7 Fed. Reg. 46, pp. 12105-12109 (3/10/2005).

[2] 38 U.S.C. §§ 4301-4333.

[3] 69 Fed. Reg., No. 181, pp. 56265-56301 (to be codified at 20 C.F.R., Part 1002).

[4] *Id.* at § 4301. USERRA replaced what was Congress' original effort to offer some measure of protection. The original provision was passed in 1940 and was named the Selective Training and Service Act of 1940, codified at 50 U.S.C. 301, *et seq.* This was replaced by the Vietnam Era Veterans' Readjustment Assistance Act of 1974, codified at 38 U.S.C. §§ 2021-2027, often referred to as the Veterans' Reemployment Rights Act.

> ***"USERRA requires employees to provide notice to their employers of their intent to take military leave…."***

[5] 38 U.S.C. §§ 4301-4333. USERRA was enacted pursuant to the War Powers Clause of the Constitution. Art I, § 8. cl. 11. Many of the other federal statutes that address employment matters have their origins in Congress' ability to regulate commerce among the states. In basing such actions on a presumption of nexus to interstate commerce, thresholds on the size of the workforce have been included within many such federal statutes.

[6] 38 U.S.C. § 4303(3) and (4).

[7] *Brandsasse v. City of Suffolk*, 72 F.Supp.2d 608 (E.D. Va. 1999) (City and director of personnel for the police department were subject to liability under USERRA as city paid the wages and controlled the hours. The director of personnel was responsible for employment actions).

[8] 38 U.S.C. § 4303.

[9] 278 F.3d 895 (9th Cir. 2002).

[10] The reserves are composed of three organizational units, the Ready Reserve, the Standby Reserve, and the Retired Reserve. *See* 10 U.S.C. § 1014(a). The training and service commitments vary depending on the nature of the reserve unit an individual serves within.

[11] 10 U.S.C. § 10149(a). *See Dow v. U.S.*, 192 F.3d 366 (2d Cir. 1999) (Ninety-six FBI agents sued, alleging that the FBI's policy prohibiting agents from serving in the Ready Reserve violated their rights under USERRA. By statute, the President is vested with the authority to screen the Ready Reserve. The president delegated this authority to the secretary of defense, who issued regulations noting that certain positions within the federal service cannot be vacated during critical times without jeopardizing the nation's security. The secretary of defense directed each federal agency head to identify "key positions" which are not to be filled by individuals in the Ready Reserve. For decades, the FBI director has determined that agents may not serve in the Ready Reserve. In reviewing this position, the Court determined that Congress did not intend for courts to interfere with determinations of this nature in the federal intelligence agencies.) For more information regarding the designation of certain federal employees as "key employees," employers should refer to regulations published at 10 C.F.R. § 44.5(b).

[12] 38 U.S.C. § 4311 (a).

[13] *Id.* at § 4311(b).

[14] *Id.* at § 3411(c). *See Fink v. City of New York*, 129 F.Supp. 511, 520 (E.D.N.Y.) (motivating factor if the employer "... took into account, considered, or conditioned its decision on that consideration."); *Sheehan v. Department of Navy*, 240 F.3d 1009 (Fed. Cir. 2001); *Gummo v. Village of Depew*, 75 F.3d 98 (2d Cir. 1996), *cert. denied*, 517 U.S. 1190 (1996) (Police officer/reservists' claim allowed to go to jury after court determined that officer established his participation in military training was a motivating factor for his termination and

sufficient evidence of animus toward reservists existed to overcome city's claim that his termination was based on grounds unrelated to his absence for military training).

[15] 38 U.S.C. § 4311(b). *See Brandsasse v. City of Suffolk*, 72 F.Supp.2d 608 (E.D.Va. 1999) (Police officer met burden necessary for case to continue against city for denying him an opportunity to take a promotional exam when he was ordered to participate in military training and retaliating against him for asserting rights protected under USERRA).

[16] 38 U.S.C. § 4311 (c)(2).

[17] USERRA was amended to create an exemption from reemployment for pre-service positions "brief and recurrent" and not likely to continue indefinitely. 38 U.S.C. § 412(de)(1)(C).

[18] 38 U.S.C. § 4313(a)(1)(A) and (B).

[19] *Id.* at § 4313(a)(4).

[20] *Id.* at § 4313(a)(2).

[21] *Id.* at § 4313(a)(4).

[22] *Id.* at § 4313(a).

[23] *Id.* at § 4312(c)(1) - (c)(4).

[24] *Id.* at § 4313(a)(3).

[25] *Id.*

[26] *Id.* at § 4312(e).

[27] *Id.*

[28] *See* Pub. L. No. 104-191 and 29 U.S.C. §§ 1181 et. seq. For more information on protections afforded reservists under HIPPA, refer to the DOL Web site at *http://www.dol.gov*, under "Frequently Asked Questions for Reservists Being Called to Active Duty."

[29] *Id.* at § 4316(a).

[30] The FMLA is codified at 29 U.S.C. § 2601 *et. seq.* The DOL issued implementing regulations located at 29 C.F.R. § 825.100 *et. seq.*

[31] 38 U.S.C. § 4312(a)(1) and (b).

[32] 38 U.S.C. § 4312(f).

[33] Pub. Law No. 108-454 (Dec 10, 2004). The notice requirement will be codified at 38 U.S.C. § 4224. The VBIA required the secretary of labor to make the text of the notice available by March 10, 2005.

[34] FR. Doc. 05-4871, p. 12108. to be published at 20 C.F.R., Appendix to Part 1002, titled "Your Rights Under USERRA."

[35] *Id.*

[36] 38 U.S.C. §§ 4321- 4322.

The Bulletin Honors

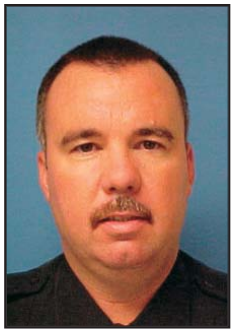
The Paso Robles, California, Police Department presents "Reward for Valor," which includes an 8-foot-tall bronze statue depicting a firefighter and a police officer rescuing a small child. Behind it stands a brick wall with the etched names of public safety servants who have lost their lives in the line of duty in San Luis Obispo County since its incorporation in 1850. Dedicated on the same day as the Paso Robles Public Safety Center, where it sits near the entrance, the monument was privately funded by individuals and businesses throughout the county.

The Bulletin Notes

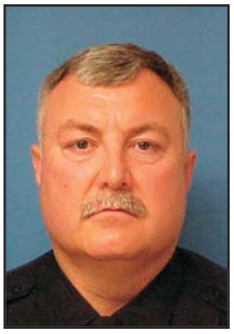
Law enforcement officers are challenged daily in the performance of their duties; they face each challenge freely and unselfishly while answering the call to duty. In certain instances, their actions warrant special attention from their respective departments. The *Bulletin* also wants to recognize those situations that transcend the normal rigors of the law enforcement profession.

Officer Johnson

While working special duty at a car show and swap meet, Officer Daniel Johnson of the Jefferson, Wisconsin, Police Department saw a person collapse near the front gate. When he got to the individual, Officer Johnson found no pulse or signs of respiration. Immediately, he checked the victim's airway and began rescue breathing. With the assistance of another citizen, Officer Johnson continued to perform CPR until the arrival of rescue personnel, who used a defibrillator to revive the individual. The victim then received hospital treatment and ultimately survived. The quick and decisive actions of Officer Johnson saved the person's life.



Officer Larsh



Officer Mast

Officers Jeff Larsh and Joel Mast of the Forest Park, Ohio, Police Department responded to a call pertaining to an attempted suicide at a residence. Upon arrival, they found the house locked. No one answered the door and the officers could not make contact with anyone inside. After receiving authorization, Officers Larsh and Mast kicked in the front door and entered the residence. Once inside, the officers noticed the smell of exhaust fumes. Officer Mast located a 4-month-old baby lying on a couch with a suicide note nearby that was written by the mother. Officer Larsh found the woman in her car in the garage with the doors closed and the motor running. The officers turned off the engine and the opened the doors. Officer Larsh moved the mother to the front yard and Officer Mast brought the child outside. The officers got medical help for the two victims and also made arrangements for the baby and mother's other three children, who had not yet arrived home from school. The quick, decisive actions of Officers Larsh and Mast saved two lives and prevented a horrible tragedy.

Nominations for the ***Bulletin Notes*** should be based on either the rescue of one or more citizens or arrest(s) made at unusual risk to an officer's safety. Submissions should include a short write-up (maximum of 250 words), a separate photograph of each nominee, and a letter from the department's ranking officer endorsing the nomination. Submissions should be sent to the Editor, *FBI Law Enforcement Bulletin*, FBI Academy, Madison Building, Room 201, Quantico, VA 22135.

U.S. Department of Justice
Federal Bureau of Investigation
FBI Law Enforcement Bulletin
935 Pennsylvania Avenue, N.W.
Washington, DC 20535-0001

Periodicals
Postage and Fees Paid
Federal Bureau of Investigation
ISSN 0014-5688

Official Business
Penalty for Private Use $300

Patch Call

The town of New Castle, New York, was founded by the Quakers in 1790. The overall shape of its police department's patch is modeled after an arrowhead. At the center is a scene depicting a Quaker and a Native American with the Hudson River in the background.

The patch of the Fort Kent, Maine, Police Department depicts a brown fort situated at the corners of the St. John and Fish Rivers with Clair, New Brunswick, Canada, in the background. The fort was established in 1839 for monitoring lumbering activities on both rivers to keep out foreign trespassers. In 1842, the St. John River became the international border.