

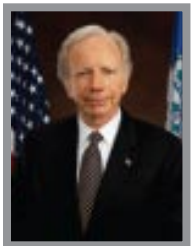
Security Magazine's Most Influential People in Security

By Diane Ritchey, Editor

They are mentors to those who work with them and for those who may be contemplating a career with the security industry. They are pioneers in their own right, as they educate, lead, advise, show the way, and ultimately, change the security industry's landscape for the better. They educate

a very anxious public about the H1N1 flu situation, develop and promote security metrics, work to prevent workplace violence and develop salary and compensation surveys for security and compliance jobs. This is Security magazine's fourth annual spotlight on the Most Influential People in the Security Industry.

Senator Joseph Lieberman (I) CT



**Chairman, Homeland Security and Government Affairs Committee
United States Senate**

Now in his fourth term representing Connecticut in the United States Senate, Joe Lieberman is perhaps best known as the Democratic candidate for Vice President in 2000. Senator Lieberman was elected to the

Connecticut State Senate in 1970 and served there for ten years, including the last six as Majority Leader. In 1980, he returned to private legal practice for two years, and from 1983 through 1988, he served as Connecticut's 21st Attorney General. He was first elected to the United States Senate in 1988. Senator Lieberman is Chairman and former Ranking Member of the Homeland Security and Governmental Affairs Committee, which is responsible for oversight of the Department of Homeland Security and assuring the efficiency and effectiveness of the Federal Government. In addition, he is a member of the Senate Armed Services Committee.

"From our 2002 work to help create the Homeland Security Department, to our implementation of the 9/11 Commission recommendations in 2004 and 2007, we have restructured agencies, programs, and lines of authority to enable the federal government to connect the dots, which it failed to do so prominently in the months leading up to September 11," Lieberman says. "At the same time, we have strengthened the capabilities of FEMA, state and local governments, first responders, and the private sector to

respond to those disasters we can't prevent, as evidenced by the Post Katrina Emergency Management Reform Act, signed into law in 2006. Recent successes in thwarting a number of terrorist plots in the U.S. demonstrate that agencies are working together far more cooperatively than the past, which leads me to believe the nation is safer today than it was eight years ago. But we have plenty of work ahead of us. As our oversight of the H1N1 epidemic and vaccine shortage proves, we cannot lower our guard against natural disasters that occur like clockwork and against a known enemy bent on destroying our Democratic way of life."

Representative Bennie Thompson (D) MS



**Chairman,
Homeland Security Committee
United States House of Representatives**

Representative Bennie G. Thompson is currently serving his ninth term as the Democratic Congressman for Mississippi's Second District. He served as alderman and mayor in his hometown for 12 years, after which he served as Hinds County Supervisor for 13 years before being elected to Congress in 1993. To begin the 110th Congress, Thompson was promoted by his colleagues to serve as the first ever Democratic Chairman of the Homeland Security Committee, a committee that was created by the U.S. House of Representatives in 2002 in the aftermath of 9/11.

As chairs of their respective committees on homeland security in the Senate and House, Sen. Lieberman and Rep. Thompson have held hearing on issues critical to the security of the United States, conducted investigations into vulnerabilities to homeland security and have worked successfully to pass numerous pieces of legislation that have had a tremendous impact on national security in the United States:

- The Post-Katrina Emergency Management Reform Act of 2006 elevated FEMA to an independent agency within the Department of Homeland Security; reversed the Department of Homeland Security's decision to separate the agency's preparedness and response functions; and strengthened FEMA's regional task forces so federal and local officials are united in their efforts and familiar with the needs of specific regions
- The Chemical Facility Anti-Terrorism Act of 2006 empowered the Department of Homeland Security to begin regulating the nation's highest risk chemical plants. It includes a provision to establish a

federal floor, not ceiling, for chemical plant security regulations. Experts have warned that a terrorist attack on one of these plants could release dangerous chemicals and put hundreds of thousands of citizens at risk.

- In 2007, Senator Lieberman led the Senate effort and Representative Thompson led the House to enact The Implementing Recommendations of the 9/11 Commission Act of 2007, which established a formula for distributing homeland security grant programs. The Act also required screening of all cargo carried on passenger airplanes within three years; gave protection from lawsuits to vigilant citizens who in good faith report suspected terrorist activity targeting airplanes, trains and buses; created a dedicated interoperability grant program to improve emergency communications for state and local first responders; and authorized more than \$4 billion over four years for rail, transit and bus security grants.

Dr. Stephen Flynn Senior Fellow at the Council of Foreign Relations



Dr. Stephen Flynn is one of the world's leading experts on homeland security and cargo security. Recently, he served as the lead homeland security adviser for the Presidential

Transition Team for President Barack Obama.

Prior to 9/11, he served as an expert advisor on homeland security to the U.S. Commission on National Security (Hart-Rudman Commission), and following the 9/11 attacks, he was the executive director of a blue-ribbon Council on Foreign Relations homeland security task force, coled by former Senators Gary Hart and Warren Rudman.

He has written numerous articles, two of the most widely-cited books on homeland security and frequently advised the Bush Administration on homeland security issues. Most recently he was asked to lead the Congressionally-mandated Quadrennial Homeland Security Review working group on transportation security, critical infrastructure protection, weapons of mass destruction and cyber security. This group will provide strategic guidance for the federal government on these issues for the next four years.

Dr. Flynn has traveled extensively abroad, where he has investigated port and container security and provided expert advice to government and industry leaders in many of the largest ports in the world.

Lynn Mattice Chairman of Security Executive Council Board of Advisors



With private sector security experience spanning 35 years, Lynn Mattice retired in 2007 as vice president and chief security officer for Boston Scientific. He previously served as director of corporate security at Whirlpool Corp., as corporate director of security at Northrop Corp. and head of security for a midcap electronics firm. He is also Chairman Emeritus of the National Intellectual Property Law Institute in Washington DC.

Nearly 35 years ago when he began his career, traditional security programs were primarily focused at gates, guns, guards and investigations thrown into the mix, he says. The "corporate cop" was the buzz phrase of the day. "Generally, unless you were in the defense and intelligence sector or the financial sector, corporate executives didn't have much for expectations of their security teams beyond being the 'corporate cop' frequently the position was even called chief of security," Mattice says. "The biggest mistake I believe we made along the way was not grabbing the title 'risk management' instead of holding on to security as an age old link to law enforcement.

"Notice that I have not referred to what we do as the 'Security Profession'...I have done that on purpose," he adds. "Some industry sectors have made significant progress in evolving the security role to one of importance and prominence in their individual corporations. However, these moves

have generally been instigated by either the individual in the role or driven by shifts in regulatory oversight that has driven the position to one of more strategic criticality to the corporation. Surprisingly, we still see 'CSOs' who are in name only."

If you ask the CEO of any of the Fortune 500 companies what the role of a CFO is or that of a CIO, Mattice says you will get a fairly consistent answer. Ask them what the role of a CSO is and see what they have to say. "Some won't even know what the term stands for. Some CEOs will tell you that the role handles executive protection and investigations. A few will tell you that the CSO plays a critical role in helping the company manage its risk profile," he notes.

Yet, he says that the security function has made significant strides. "I believe, however, that until security executives truly focus on adding value, taking on the tough assignments and aligning with the corporation's needs and goals we will have an even harder time getting there," says Mattice.

John E. McClurg Vice President, CSO, Honeywell's Global Security Organization



He's one of the best leaders in the industry. At Honeywell, McClurg is responsible for the strategic focus and tactical operations of Honeywell's internal global security services, both physical and cyber. He is charged with the advancement of business continuity, the seamless integration of Honeywell's various security offerings, and with improv-

ing the effectiveness and efficiency of security initiatives. He also serves on Honeywell's Technology Leadership and IT Councils.

He has led the effort to measure security's role in an organization. Metrics, he says, is not new, yet, "They are ways to relate to the business. It's the perfect method to show your indispensability to the enterprise," he says.

His background includes vice president of Global Security at Lucent Technologies/Bell Laboratories and in the U.S. Intelligence Community, as a twice-decorated member of the FBI, where he held an assignment with the U.S. Department of Energy (DOE) as a Branch Chief charged with establishing a cyber-counterintelligence program within the DOE's newly created Office of Counterintelligence. Prior to that, he served as a Supervisory Special Agent within the FBI, assisting in the establishment of the FBI's new Computer Investigations and Infrastructure Threat Assessment Center or what is today known as the National Infrastructure Protection Center within DHS. McClurg also served, for a time, on assignment as a deputy branch chief with the Central Intelligence Agency, helping to establish the new Counterespionage Group and was responsible for the management of complex counterespionage investigations.

He was named a 2008 CSO Compass Award recipient; holds a J.D. degree from Brigham Young University, is a member of the Utah Bar Association, and sits on both the Executive Working Group of the Overseas Security Advisory Council of the U.S. Department of State and on the FBI's Domestic Security Alliance Council.

Richard Lefler Dean of Emeritus Faculty for the Security Executive Council



From the beginning of his career, Richard Lefler recognized the importance of executive leadership skills in all aspects of an organization, including security. He attended the Federal

Executive Institute for Executive Education Program in 1981 and the John F. Kennedy School of Government's Program for Senior Managers in Government at Harvard University in 1982.

He retired as the vice president for worldwide security at American Express in 2001. He was also deputy special agent in charge

of the U.S. Secret Service's New York office, where assignments included special agent in charge of protective operations, the Presidential Protective Division and the Vice Presidential Protective Division. Since his retirement, Lefler has continued to improve the state of security in the public and private sectors, particularly in global security management, financial product fraud protection, executive, employee and facilities protection and investigative coordination with federal, state and international government.

"Business leaders are demanding security leaders understand their business models, and as a result, larger numbers of security leaders are coming from the business side of the company," he says. "This trend will continue."

Jim Hutton Chief Security Officer, Director of Global Security, Procter & Gamble Company



Jim Hutton is responsible for worldwide security direction and consultation for all business units of a multi-billion-dollar enterprise that includes several icon brands. With

the support of Procter & Gamble's Global Security Leadership Team, Hutton developed a strategic plan that includes robust performance metrics related to security.

His past experience also includes vice president and chief security officer for the Gillette Co., and with the U.S. State Department's Bureau of Diplomatic Security, where he protected diplomatic personnel, information and facilities around the world.

"When I began my career in security in 1984 as a Special Agent with the U.S. Department of State's Diplomatic Security Service, our responsibilities were very traditional: protect people, assets, facilities, and information, along with various investigative taskings," he says. "Although we were a government organization, our mission was similar to what was expected within the industry – albeit in a much different context – the secure conduct of U.S. international affairs. Planning and execution activities were somewhat predictable and results were usually viewed in a subjective manner by local supervisors within a historically acceptable range. This resulted in a reliable, consistent, and practical level of protection

provided to our parent organization."

As he moved to the private sector, it quickly became apparent to him that the security function needed to do a better job of customizing processes and contributions to meet specialized needs in all company functions. "One size no longer fits all and mere loss prevention or protective activities weren't enough to meet the company's security needs," he says. "Performance metrics became more important, and developing strong security talent that could relate to the business was paramount."

"Pace has quickened, stakes are higher, and impacts are more immediate," he notes when thinking about the future. "We now need to appropriately employ our time-honored skills and learn new ones to operate in a VUCA world – a world that is volatile, uncertain, complex and ambiguous."

George Campbell Security Executive Council Emeritus Faculty



To promote his "pet cause" of security metrics, George Campbell has authored "Measures & Metrics in Corporate Security – Communicating Business Value" for

the SEC and is the SEC practice leader on Security Program Measurements and Analytics and chairman of SEC's Security Metrics Working Group.

Campbell retired in 2002 as chief security officer (CSO) at Fidelity Investments, the largest mutual fund company in the United States with more than 32,500 employees.

"I started in this business when physical security from a technology standpoint was hardwired, analog, basic security video, alarm annunciation and access control – ancient stuff compared to the integrated, on-board intelligence we see today," he says. "Management expectations were far more traditional in terms of the risk profile assigned to our portfolio. The Embassy, WTC and Omaha bombings re-wrote the book on physical security and the increasingly sophisticated (and globally outsourced) insiders and data security threats forced our notions of defense in depth. Then, 9/11 and corporate scandals created the new paradigm of regulatory and standards compliance and a higher boardroom visibility for the CSO."

"We now find ourselves competing with

an economy that demands to-the-bone contributions as a good corporate citizen while concurrently staring at a broader and more diverse global threat spectrum,” he notes. “All non-core business functions are under pressure to demonstrate alignment with, and value to, the evolving business strategy; the conduct of internal controls are potential targets of reductions in force, and what we once knew as ‘the company’ may now be a confederation of contractual relationships with no clear ties to our culture of integrity and corporate security. In my view, the landscape of corporate asset protection is in transition.”

Yet, he says, “Our challenge as leaders is to position our programs squarely within the enterprise risk management strategy, to be seen as providing products and services that enable the business to do what would otherwise be too risky.”

Thomas J. Mahlik

Deputy Assistant Director of Counterintelligence for Naval Criminal Investigative Service (Previously detailed to FBI’s Directorate of Intelligence as Chief Domain Management, FBI HQ)



Under Tom Mahlik’s leadership, the FBI’s Domain program has had a galvanizing impact on the way the USG (Law Enforcement, Counterintelligence and Intelligence) col-

laborates with the private sector to thwart myriad diverse threats. Specifically, the program has resulted in early detection, stronger preventive postures and an agreed-upon framework of responsiveness by USG to private-sector referrals.

Mahlik has helped reinvigorate partnerships across the industry that has enabled more transparency between security industry leaders and the FBI at the local and regional levels. He has created FBI (and USIC) outreach programs in conjunction with the security industry to build awareness and create dialogue, resulting in a number of national conferences/seminars to build protection strategies, create tripwires and renew communication avenues.

He has championed the “know your domain” concept across the FBI and across the USIC as the centerpiece in the transformation of the FBI intelligence program. A

key part of this effort has been coordinating the outreach activities of the FBI to ensure the right messages are being delivered on a timely basis that meet the core requirements and expectations of private-sector constituents.

He’s learned that, “While the complexities of our jobs in the security industry would naturally include a comprehensive triage and understanding of current and emergent threats, I am increasingly sensitized to the fact that our understanding of threat/vulnerability issues, however deep, are only as good as the holistic understanding we must also have in the context of corporate objectives and the business environment, not to mention the increasing premium placed on abilities to communicate real solutions – often, timely and creatively – to ‘the decision maker’ that leads to smart action.”

Today, he says, it’s all about partnerships. “To comprehensively ‘win,’ we must mobilize the security industry towards new paradigms, new dialogue, new partnerships, new means/modes of information exchange and new problem-solving approaches with (and between) the government and the private sector. Strategic forums that lead to more congenial communication, strong awareness and decisiveness in managing risk, must be championed and pursued.”

Francis J. D’Addario

Security Executive Council Emeritus Faculty



Francis D’Addario has led his life endeavoring to protect people, secure assets and contribute margin for global markets. As a former vice president of Partner and

Asset Protection for the Starbucks Coffee Company, director of security for Jerrico Inc. and as regions manager for the Southland Corp., he has benchmarked innovations and results, including returns on investment from global mitigations of physical, logical and fiscal risks.

“I began my career shortly after the U.S. bicentennial in Washington D.C.,” he says. “As an avid student of security I was both influenced and consternated by alleged ‘best practices’ that were often offered with little data. Economics clearly informed prevention investment. One arguable example was the superpowers nearly bankrupting themselves before settling on the more afford-

able course of ‘trust but verify.’ Security was a prized but elusive objective that only seemed reachable in measured steps.

“My path to all-hazard risk mitigation led me to data sets that were persuasive for protecting people, securing assets, and contributing to the net profitability of my mentors or patrons year over year. My epiphanies beyond ‘trust but verify’ diligence included crime prevention through environmental design, exception-based reporting, and just-in-time security with relevant metrics. The ‘people, process and technology’ benchmarks my teams begged, borrowed, or adapted with innovation, served up credible risk mitigation and return on investment results. More importantly they influenced protection practices for larger communities including small business associations to global trading partnerships.

“We are presently faced with a myriad of human health, logical, and physical hazards posed by man and nature,” he adds. “Our legacy as risk mitigators will be determined by our preparedness at home, in the institutions we influence and the communities in which we live.”

John Martinicky

Director of Security, Navistar Corp.



John Martinicky has been in security for more than 25 years, working his way up the ranks to his current position as the director of Security for Navistar, Inc a fortune 500 compa-

ny with 15,000 employees. Martinicky is on the job 24/7, handling the day to day security needs of the company and ensuring that company employees feel safe and secure, that theft remains in check, in addition to handling internal investigations when something goes wrong.

He’s seen many changes in the industry. “This industry has evolved into where we, as security directors, are integrated into the business, contributing to the business, and touching all different business functions, such as pre-employment, drug testing, due diligence on potential business partners and risk assessments for emerging markets.”

Martinicky was one of the first to require drug hair testing for Navistar, which has saved the company millions of dollars. He was one of the first to streamline the background check process and reduce the

amount of wait time for new hires and more accurately identify applicant inconsistencies. Martinicky's metrics program collects and analyzes information on almost everything his department does. He uses this data to show his department's worth to key executives, which in turn, provides the funding for additional programs or improvements to existing programs. He understands the value of technology and is constantly looking for ways to provide value to the security function. For example, he recently recognized that computer forensics is expensive to outsource, so he found a way to develop the expertise in-house. This is saving Navistar almost \$100,000 per year.

Of his accomplishments, he says, "There used to be times that I would say my accomplishments are successfully concluding an investigation. As time has gone on, I'm more proud of the fact that our security executives have improved their educational level – a number of them have CPPs and MBAs. Security is more respected within the company. Most importantly, our employees feel safe when they work here and when they travel.

Martinicky also continues to improve himself through various industry certifications, speaking engagements, and recently, his MBA. He also serves on Security's Editorial Advisory Board.

Susan Pohlman Business Manager, International Security Management Association (ISMA)



Twenty-five years ago a young international association of top-level security executives approached Susan Pohlman to utilize her accounting and business experience to manage it.

Pohlman eventually built the International Security Management Association (ISMA) into an effective professional organization.

As business manager of ISMA, Pohlman provides and support an international forum for select security executives whose combined expertise can be used to develop, organize, assimilate and share knowledge and to enhance professional and business standards.

"I became involved with a profession that was new to me, intriguing and providing the potential for unique challenges," Pohlman says. "But several areas I did know some-

thing about were client service, the value of networking and the power of relationships and information sharing. I soon discovered this was the key that would overcome some of the obstacles facing security directors who had limited relationships with others in the profession.

"The security profession is not unique in the premise that information is the key to success," she continues. "But security executives do rely much more heavily on the ability to benchmark with other companies, including competitors, on critical risk management strategies.

"Going forward, it is critical that we provide the contacts and educational tools for the next generation of CSOs," she says.

R.E. "Sandy" Sandquist Director of Global Security, General Mills



are the most important problem for them at that moment and they deserve my full attention," says R.E. "Sandy" Sandquist. "We are all confronted with serious security concerns at a new level and are having a more significant impact to the businesses that we serve than ever before. Yet, it is important to never forget the honor that we are given by having the opportunity to help someone."

As director of global security for General Mills, Sandquist has aligned his security team and strategic initiatives with the company's business objects in a way that has put him among the top leaders in his profession. Sandquist drives the concept of managing domestic product diversion that has resulted in a program now saving millions of dollars.

Sandquist provided security for an intelligence-gathering unit while serving in the U.S. Air Force. At the end of the Vietnam War, he served as a police officer for San Angelo, Tex., before beginning a corporate security career that would include GTE, U.S. Sprint and Pillsbury as well as General Mills.

"Many years ago when I began my career in corporate security the focus was on physical security: lock and key plans, fences, access control, identification of employees and guard management," he says. "Many

security leaders of the time were starting a second career after years in law enforcement or the military, and many business partners were certain that the security director lurking in the background had the ability to extract a confession by his mere presence or certainly had a network of contacts in mysterious agencies from around the world at his beck and call. While there may have been a grain of truth in this belief, the security world is incredibly different today."

Today's security leader must seek out ways to focus security strategy in our global economy, he notes. "It is essential for today's security leaders to have a seat at the enterprise risk management table in order to understand the risks their business faces. Understanding and mitigating business risk brings clarity to the purpose of corporate security and diminishes the need to articulate value," he says.

Michael R. Cummings Director, Loss Prevention Services, Aurora Health Care



Michael R. Cummings began in retail security in 1973 as a part-time job to get him through his last year of college. He decided to take the proverbial "year off" to save some money before going on for a higher degree. Yet, his part-time job turned into a career before he knew it. After spending the first 12 years in the retail sector, he joined Aurora Health Care as assistant director of security. At the time, he says, "I felt I had a solid understanding of security in general, but knew that I did not know much about this 'vertical market.'" Shortly after, he sat for and passed his CPP. Today, he is director, Loss Prevention Services for Aurora Health Care.

He still feels strongly about certification: all of his security staff must become certified security officers under the IAHS program as a condition of employment.

The security industry has matured since 1973, he says. "We understand that we are not as earlier perceived, simply a 'necessary evil,' but rather an important internal resource to our companies," he adds. "This has come about as we became proficient not only about the operational responsibilities that we have always had, but understood the business side of whatever vertical market in which we practice our profession. This has

given us more access to the 'C' suite and the top decision makers in our organizations, which has allowed us to have the type of positive impact not always previously available. This is an area where we are just scratching the surface."

He's also seen more of an emphasis on creative partnerships. "Examples of traditional security groups working with groups as diverse as safety, human resources, IT and even public law enforcement groups on everything from legislative and educational to standards and guidelines are examples of that dynamic. I see this as a positive and a necessity and feel we will see more of these efforts as we realize that we are all in this together and resources are too scarce to go it alone."

Radford Jones, Jerome Miller, Brit Weber

**Leaders of Michigan State University's
Critical Incident Protocol program**



Building on a groundbreaking security administration curriculum, the School of Criminal Justice at Michigan State University (MSU) in 1998 began researching the effectiveness and practicality of government and business working together for joint crisis management. In 2000, MSU published the Critical Incident Protocol guide, which became a guide for government agencies, businesses and non-profits to build their partnership programs. In 2002, the Critical Incident Protocol (CIP) – Community Facilitation Program was launched; it was



federally funded and offered free to communities. Radford Jones, formerly manager of security and fire protection at Ford Motor Company and now an academic specialist in the MSU School of Criminal Justice, founded the program. Jerome P. Miller, formerly executive in charge of International and Special Security Operations for Daimler Chrysler Corp., is CIP program consultant.

The program director is Brit Weber, who served 28 years with the Michigan State Police in the Uniform Division and served as part of the United Nations Peace Keeping Mission in Kosovo.

To date, MSU has initiated public/private partnerships with 47 communities in 24 states and with more than 4,200 public and private sector leaders participating in CIP program workshops.

As the program director, Brit Weber speaks across the nation on the importance of building public/private partnerships for joint crisis management. "The future security professional will include more education, improved business management acumen, use of more project management processes, integration with business continuity and risk management practices, expansion of security network of collaboration and making sure the components of security management are embedded throughout the organization," he predicts.

Miller entered the private security industry in 1986 after a career in law enforcement, and says that this was a period of advancement and recognition for the industry. There was a movement to professionalize the ranks of security supervisors and managers through accreditation programs such as the CPP certificate. In addition, some universities were offering degrees in security management.

"There has been an industry-wide response to the terrorist attack on 9/11, with more sophisticated physical security systems designed to protect the workplace," he shares. "And, there has been a significant change in the working relationships between the private sector and the public sector. Information regarding threat levels, targets, etc. is now being shared on a regular basis."

In 1983, Jones retired from the U.S. Secret Service and joined the global Security and Fire Operations of Ford Motor Company. The Secret Service mission of protecting the President can only be accomplished through support from other law enforcement agencies and community entities visited. "Upon joining the private security ranks I was surprised about the lack of strong partnerships with internal company components and external public agencies," he says. "Within private security there was a philosophy: 'We are the company cops, know how to do it best and keep it a secret.'"

This "Do it on your own" philosophy was counterproductive. "I believed that it was important to develop strong working relationships with other key company components, such as the audit, legal and finance staffs," he says. "I engaged in a walking

around management approach to develop important personal and professional links with other key managers in the company."

Dr. Anne Schuchat

Director of the Center for Disease Control (CDC) National Center for Immunization and Respiratory Diseases



"Public service is a privilege. For me it has also been a joy." As director of CDC's National Center for Immunization and Respiratory Diseases, Dr. Anne Schuchat

is at the forefront of the CDC's H1N1 response. She is in briefings, webcasts and outreach sessions almost daily, and she is one of the most prominent faces of the response to H1N1 flu. It is her job to encourage acceptance of the vaccine while reducing anger about its late arrival; to raise awareness; to convey what researchers are learning about this flu; to manage skepticism, confusion, fear, paranoia; and to answer questions.

Prior to her current appointment, she served as the director of CDC's National Immunization Program; acting director of the National Center for Infectious Diseases (NCID); chief of the Respiratory Diseases Branch at NCID; and as the initial medical director of the Active Bacterial Core surveillance Emerging Infections Program Network, a multi-state collaboration between CDC, state health departments and academic institutions that tracks invasive bacterial infections, informs vaccine and prevention policy, and monitors program impact.

Charles P. Connolly

**Security Executive Council
Emeritus Faculty**



"It's been 52 years since I began my career in the public and private protection profession," says Charles P. (Charlie) Connolly. "I have observed an incremental progression

of recognition and partnership between the police and security professions. Policing considered itself independent, highly pro-

rective of turf and suspicious of private sector motives and standards of performance.”

That was then; it is no longer the case now, he says. The process of cooperation and recognition, while not perfect, has vastly improved particularly in the United States and increasingly so in Europe and other parts of the world. Why? “Perceptions among law enforcement have changed,” he says. “The crossover of second careers towards private security in an industry that dwarfs public protection two and three times its size obviously enhanced a better understanding of what private security does and can do to keep this nation safe. I have witnessed the melding of a greater understanding of the need for a mutual partnership pact. This will continue.”

Connolly’s public and private protection career includes vice president/director of world wide security for Merrill Lynch, where he was responsible for the physical security of more than 68,000 employees assigned to 980 buildings in 44 countries and 50 states.

Tony Castorino

Director of Physical Security, Technicolor



Tony Castorino’s security career began working as a contract guard at Technicolor, a provider of production and post-production services to the motion picture, broadcast and cable industry. He’s

now director of physical security.

“When I first started in the industry, security was basically a guard that watched the entrance of a facility and occasionally went on guard tour rounds,” he says. “If there were security cameras, their images were black and white and displayed on a small 7-inch monitor with no recording available.

“Through maturation of security cameras we gained the ability to record on a 24 hour VCR,” he says. “With this system you had to remember to change the tapes daily and storage took up a lot of room in order to maintain a 90-day requirement of tape. From there we moved to the DVR technology, allowing us the ability to watch video that was digitized and no longer had to store hundreds of VCR tapes. With the introduction of the IP cameras, the product is fully digital and the storage costs have greatly been reduced.”

He sees his greatest accomplishments as

design and implementation of all security controls for several new buildings, including Technicolor’s new Hollywood facility. Castorino was tasked with selecting the facility’s video surveillance system, as well as overseeing its installation.

A large part of his job also includes protecting intellectual property. Each year, billions of dollars in intellectual property passes through the hands of the staff at Technicolor.

John Piper

Security Executive Council Subject Matter Expert Faculty



more than 70 countries.

John Piper, retired from the U.S. Secret Service, became vice president, Special Projects Sector, for Scientech Engineering before serving as manager of global security engineering and risk management for ExxonMobil Corp. Now a technical consultant, he has also been an adjunct faculty member at George Washington University.

“Twenty five years ago the security industry was relying on security surveys and checklist techniques to make many, if not most, security decisions,” he says. “One of my mentors – Roger Mattsen, PhD – used to say ‘a survey or checklist is a sure fire way to learn more and more about less and less.’ There was a need for high-end security decision making tools.” Also, he says, there was a shift away from the complex quantitative risk assessment methodologies to efficient, less costly qualitative models.

In the mid-1990s, the qualitative models were evaluated by GAO for applications in counter terrorism and cyber security decision making and resource allocations. One later example: DHS developed a qualitative tool (the Chemical Security Assessment Tool or CSAT) for application to expectations of the 2006 Chemical Security Act.

“There is a need for high quality decision making on a much broader scale than currently exists,” Piper contends. “DHS has identified about 17 sectors that comprise our critical infrastructure. The CSAT and other qualitative models should be applied

to those sectors.” The result: optimized security processes, technology applications, and a connection between tactical risk assessments and strategic risk management.

Erroll G. Southers

USC School of Policy, Planning and Development



How many students at USC can say their professor was a former FBI special agent? SPPD alumnus Erroll Southers (MPA ‘98) returned to USC with three new identities: professor on counter-terrorism, founding member of the SPPD Alumni Association, and associate director of the USC Homeland Security Center for Risk and Economic Analysis of Terrorism Events. As of press time, he was a nominee for head of the TSA.

“I lived in that world where the CIA, FBI, customs and police didn’t share information and were extremely competitive with each other – it was a big mistake,” Southers says. Southers worked four years for the FBI – three of those years as a member of SWAT – completing 41 missions all over the U.S. He was also a Santa Monica Police Department detective, where his experience qualifies him to be a gang and security expert witness, and a member of the Rio Hondo Police Academy.

Since 2003, Southers has taught a master’s-level “Homeland Security and Public Policy” class, which is structured on the contemporary discourse of terrorism post-September 11.

In his early years Southers first crossed paths with Governor Arnold Schwarzenegger – as competitive body builders. The governor eventually appointed Southers as the deputy director of the California Office of Homeland Security. These days, both are too busy to go motorcycle-riding every Sunday like they used to, so Southers has sought alternate forms of exercise. “I get my best ideas while cycling from the Marina to Palos Verdes,” he says.

Southers’s recommendations and analysis help protect the fifth largest economy in the world, and he believes that best way to defend against terrorism is to be better prepared for all disasters, by engaging the public in an ongoing education process.

“I’m not paranoid and I’m not a fear monger, but I am a realist and I know what the threats are,” Southers says. “If you think about it, the better prepared we are

to respond to an earthquake, the better we will be able to mitigate a terrorist attack or recover from a natural disaster.”

Steve Walker

Security Executive Council Subject Matter Expert Faculty



Steve Walker has created the only certified salary and compensation survey for security and compliance jobs, enabling compensation levels for security professionals to

be based on solid numbers and benchmarks rather than on information adapted from jobs in other disciplines.

Walker has more than 18 years in management consulting. He is a senior partner of the Foushee Group and a member of the SEC's Content Expert Faculty, where he helps develop strategic security services and products for council members.

The Foush e Group had been contemplating conducting a security survey for some time prior to 9/11, he says. “We recognized though client contacts, that there may have been a need to produce a survey specific to the security function for a couple of reasons. The first being, a need for companies to receive accurate compensation information on security positions, second is that there was not a survey that was specifically targeted to the security field. The market need, and 9/11 spurred us into action, to commit the resources and time and to produce a new survey.” The resulting Security & Compliance compensation survey is specific to the security industry, providing reliable market information on security positions to gauge their market value.

Ernie Allen

President and CEO, International Centre for Missing & Exploited Children



Under Ernie Allen's leadership, the International Centre for Missing & Exploited Children has built a global network that includes 17 nations and is leading the effort to create new missing and exploited children's centers

around the world. More than 140,000 children have been recovered by the organization, and it has increased its recovery rate from 62 percent in 1990 to 97 percent today.

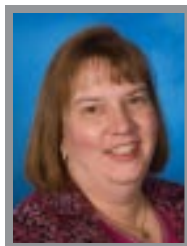
He also has brought technology and innovation to the organization, including age progression and forensic imaging of long-term missing children, a 24-hour missing children hotline and training for more than 253,000 law enforcement officers. He established the CyberTipline, a 9-1-1 for the Internet, which has resulted in thousands of successful prosecutions, and launched a new unit to help the U.S. Marshals track down more than 100,000 fugitive sex offenders.

“Time is the enemy in the search for a missing child,” he says. “Yet, police departments had mandatory waiting periods before they would even take a report. We worked with Congress to eliminate the waiting periods by law and require every police department to take an immediate report and immediately enter that report into the FBI's national crime computer.”

Technology is key, he says. “We have built networks, shared information and harnessed the power of technology to change the way America provides security to its children and families.”

Margaret Spaninger

Senior Associate, Booz Allen Hamilton



Training innovation and integrating security with business processes have been the passion of Margaret Spaninger's 30-year career in the information technology sector. She began her IT career in the early 1980s as she progressed through the ranks of Honeywell's Federal Systems Operations group as a trainer and instructional design expert. Spaninger has spent the last 15 years at Booz Allen Hamilton working with federal agencies in the intelligence, defense and civil sectors.

Spaninger champions the security awareness and training cause and believes that, “good training doesn't happen by accident.” At Honeywell, she built curriculums from reusable learning objects, which saved development time and resources. Since joining Booz Allen, she has focused her efforts on workforce assurance – building a security-aware workforce and culture. She is a

driving force behind role-based, enterprise-centric security training and one of the primary thought leaders behind “professionalization,” which helped move the security job from a collateral duty assignment to a full-time position in the federal sector.

“Today's IT security environment is characterized by change, complexity and speed,” she notes. “Enterprises around the world are charged with securing their information and information assets. I believe this responsibility ultimately falls to the information technology and security practitioners within an organization, who must not only know, understand and be able to apply fundamental security concepts, but also the specific security policy and procedures of their organization.”

“Few enterprises have sufficient training programs and resources that are focused on the specific material weaknesses of their security programs,” she continues. “Security awareness and training are effective countermeasures that are often neglected for more glamorous and tangible hardware and software solutions. Yet, a blended solution can be used to advance the security cause and integrate security practices with standard business processes.”

Norman R. Bottom Jr., Ph.D.

Author, Educator, Mentor



He influenced thousands, visibly improved the profession, encouraged and mentored people in and out of security as well as personally touched scores of men and women with his wit and wisdom, before he passed away in early August.

Dr. Bottom's career began more than 40 years ago while conducting and directing research with the Defense Intelligence Agency. He designed and staffed one of the first master's degree programs in security at the university level, and taught graduate and undergraduate courses on diverse topics. He held numerous certifications, including the Certified Security Trainer (Emeritus), Certified Protection Officer, Certified Protection Professional and Certified Personal Protection Specialist.

Always the teacher, “Bottom served as chairman of the International Foundation for Protection Officers (IFPO) in its early stages. His contributions and powerful lead-

ership qualities lead IFPO into a very favorable position in the security education and training sector,” says Sandi Davies, the foundation’s executive director. “Dr. Bottom had incredible vision and a determination to make a difference in the security industry.”

A prolific writer, he has authored and reviewed numerous articles and is the author of the book “Security/Loss Control Negligence;” co-author of “Industrial Espionage: Intelligence Techniques and Countermeasures;” and author of the “Parking Lot and Garage Security Handbook.”

Bottom’s influence lives on with educational projects and programs; associations and foundations; and through clear and useful books and articles.

Barry Nixon

National Institute for Prevention of Workplace Violence, Inc.



The statement “an ounce of prevention is worth a pound of cure” was never truer when considering that an average of approximately 1,000 people annually have been killed on the job since 1990, up from an average of 750 in the 1980s.

Since 1994, Barry Nixon has worked to decrease workplace violence. Nixon is founder of the National Institute for Prevention of Workplace Violence, Inc., which serves as a center for research,

consulting, training and communication. Its mission is to educate employers, unions and employees about the growing threat of violence in the workplace and how to effectively deal with it. Nixon is also creator of the web site —www.Workplaceviolence911.com, which provides information on the subject. Nixon coined the term “Infinity Screening,” which has now become part of the lexicon of background screening terminology.

“It’s no secret that the tragic events of 9/11 bolstered the focus on security when terrorism found its way to American soil,” he says. “Since then the profession has started to mature and made giant steps toward becoming real business partners with demonstrated value added to the enterprise.”

Andrew B. Serwin

Founding Chair of the Privacy, Security & Information Management Practice

Partner in the San Diego law office of Foley & Lardner LLP



Attorney Andrew Serwin has been on the cutting edge of information security and privacy issues from a business and legal perspective. He serves on the privacy and the legal subcommittees of the Privacy & Security Advisory Board of the California Health and Human Services Agency by the California Office of HIPAA Implementation.

“When I first began practicing in this area, there was a lack of understanding regarding the importance of information, as well as the potential brand impact of security incidents,” he says. “Terrorism prevention was not a focus for most private companies; rather, the focus was stopping the one-off hacker who sought to crack a system, in many cases just to show it could be done. Privacy was not seen as a ‘bet the company’ issue and security breaches were almost never announced to the public.”

That has changed. “Legal compliance is often the primary goal of protecting information, but brand protection is also a major concern now,” he says. “Moreover, while hacking still occurs, more is state-sponsored cyberterrorism, and this means that companies and governments must be increasingly vigilant against coordinated attacks.” **SECURITY**

The Most Influential People in Security, 2009

Senator Joseph Lieberman (I) CT

Chairman, Homeland Security and Government Affairs Committee
United States Senate

Representative Bennie Thompson (D) MS

Chairman, Homeland Security Committee
United States House of Representatives

Dr. Stephen Flynn

Senior Fellow at the Council of Foreign Relations

Lynn Mattice

Chairman of Security Executive Council Board of Advisors

John E. McClurg

Vice President, CSO, Honeywell’s Global Security Organization

Richard Lefler

Dean of Emeritus, Faculty for the Security Executive Council

Jim Hutton

Chief Security Officer, Director of Global Security, Procter & Gamble Company

George Campbell

Security Executive Council Emeritus Faculty

Thomas J. Mahlik

Deputy Assistant Director of Counterintelligence for Naval Criminal Investigative Service (Previously detailed to FBI’s Directorate of Intelligence as Chief Domain Management, FBI HQ)

Francis J. D’Addario

Security Executive Council Emeritus Faculty

John Martinicky

Director of Security, Navistar Corp.

Susan Pohlman

Business Manager, International Security Management Association (ISMA)

R.E. “Sandy” Sandquist

Director of Global Security, General Mills

Michael R. Cummings

Director, Loss Prevention Services, Aurora Health Care

Radford Jones, Jerome Miller, Brit Weber

Leaders of Michigan State University’s Critical Incident Protocol program

Dr. Anne Schuchat

Director of the Center for Disease Control (CDC) National Center for Immunization and Respiratory Diseases

Charles P. Connolly

Security Executive Council Emeritus Faculty

Tony Castorino

Director of Physical Security, Technicolor

John Piper

Security Executive Council Subject Matter Expert Faculty

Erroll G. Southers

USC School of Policy, Planning and Development

Steve Walker

Security Executive Council Subject Matter Expert Faculty

Ernie Allen

President and CEO, International Centre for Missing & Exploited Children

Margaret Spanninger

Senior Associate, Booz Allen Hamilton

Norman R. Bottom Jr., Ph.D.

Author, Educator, Mentor

Barry Nixon

National Institute for Prevention of Workplace Violence, Inc.

Andrew B. Serwin

Founding Chair of the Privacy, Security & Information Management Practice and Partner in the San Diego law firm, Foley & Lardner LLP