A PUBLICATION OF THE INSPECTORS GENERAL OF THE UNITED STATES

The Journal of Public Inquiry

FALL/WINTER

2012-2013

COUNCIL OF THE INSPECTORS GENERAL ON INTEGRITY AND EFFICIENCY

Journal of Public Inquiry

Council of the Inspectors General on Integrity and Efficiency

ꕥ Denotes the end of an article.

The Role of the Office of Inspector General in Identifying Risks at a Government Agency

By Inspector General Richard Moore and Ben Wagner

In this article, we examine the intersection of federal agency responsibility for accurately assessing and dealing with risks to the agency and the role of the Inspector General in this important area. When the inevitable, "Where was the IG?" comes after an agency crisis, we should have a good answer. Was the risk that resulted in a crisis on the IG's radar? If not, why not? The role of the IG, as we discuss here, is not to supplant the agency's responsibility to properly identify and control risks but to accurately assess the sufficiency of the agency's risk management program and to identify risks not recognized by the agency as appropriate. If the agency's enterprise risk management program is comprehensive, the IG can rely with some confidence on the program to allocate scarce OIG resources for focused audits, inspections and investigations.

"In the past, many companies focused risk identification on past losses, failures and incidents."

GETTING IT ON THE RADAR: DEVELOPING A ROBUST ENTERPRISE RISK MANAGEMENT PROGRAM

In today's world, how effective a business or government agency is at identifying its risks and taking action to reduce those risks can be the difference between success and failure. Managing risk is a challenging endeavor. In the past, many companies focused risk identification on past losses, failures and incidents. Today, companies and government agencies are well advised to actively seek out the unknown and identify what process deviations are occurring and what negative workforce behaviors are occurring throughout the organization now that could create a significant risk, or more importantly, what small deviations when added together could constitute a significant risk for the company. Deviations from both organization-approved standardized processes and established workforce behaviors must be caught in the risk management net early.

There are many reasons an ERM program might be ineffective, but two common causes are (1) the agency or company's organizational health or culture, and (2) the design of the ERM program. If either of these components is weak, the chance of missing serious risks increases exponentially.

THE ROLE OF CULTURE IN DEVELOPING AN ERM PROGRAM

Private sector companies routinely pay consultants millions of dollars to design a "state of the art" ERM program only to see them fail. The best-designed risk management program is destined to fail if the culture of the organization does not make it safe for employees at all levels to raise risks. If employees hear the words, "We want you to raise risks you see in your work area," but what they see does not support those words, then the double message results

"Management should be able to depend on employees to take responsibility for identifying risks."

in a culture that does not support "raising your hand." Managers who see other managers fired or moved because they offered a position that conflicts with upper management will quickly recognize talk about "risk management" as simply that—talk. The key is creating a safe environment where differing opinions can be shared in a mutually respectful manner.

Communicating priorities so that employees know they have been heard, whether their ideas are followed or not, engenders trust in leadership and a willingness to "raise your hand" again. Recruiting employees at all levels of an organization is critical for an effective risk management system. Relying on only leadership (executives and managers) often robs the system of the observations of those closest to the risks. A culture in which employees believe they can safely have awkward conversations about policies and practices is fundamental to an effective risk management system. Identifying risks must become a normal part of every employee's work life. For the "new normal" to take hold, however, there must be a trust that identified risks will be fairly evaluated without retaliation. Few government or corporate leaders, however, have the expertise to create that environment without specialized assistance from professionals who can objectively test the culture of an organization and take steps to improve the culture as required. Therefore, those organizations that have poor organizational health are most vulnerable to unforeseen risks.

Creating a safe environment for employees to raise issues comes with a corresponding duty of employees to follow clear behaviors set by the organization. In other words, there must be a corresponding duty of employees to be accountable when management creates a safe environment to proffer differing opinions. This is more than simply requiring employees to follow policies and procedures or to avoid engaging in unethical or illegal behavior. The organization should have a list of desired behaviors that reflect the culture the organization aspires to have. These behaviors may include such things as give and expect mutual respect, communicate expectations clearly, seek and value the opinions of others and be comfortable bringing up issues and recommending solutions. Management should be able to depend on employees to take responsibility for identifying risks. As the "new normal" takes hold, risk identification and reduction will become part of everyone's job.

THE IMPORTANCE OF THE RIGHT DESIGN FOR AN ERM PROGRAM

In addition to culture, the appropriate design of the risk management program is critical. The Committee on Sponsoring Organizations[1] defines ERM as "…[a] process, effected [sic] by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite to provide reasonable assurance regarding the achievement of entity objectives."

According to COSO's framework, a mature ERM program has risk management embedded in how the organization conducts business. Executives and line management comprehend and recognize the value of the program. Dedicated risk management resources are consulted by executive/operational lines for risk advisory support and recognized as a strategic business driver.

According to the COSO report, enterprise risk management enables management to effectively deal with uncertainty and associated risk and opportunity, enhancing the capacity to build value. The COSO report also states management can

1) In September 2004, Committee of Sponsoring Organizations of the Treadway Commission issued Enterprise Risk Management–Integrated Framework. The executive summary can be found at http://www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf.

maximize value by setting strategy and objectives to strike an optimal balance between growth and return goals and related risks, and efficiently and effectively deploying resources in pursuit of the entity's objectives. Enterprise risk management encompasses:

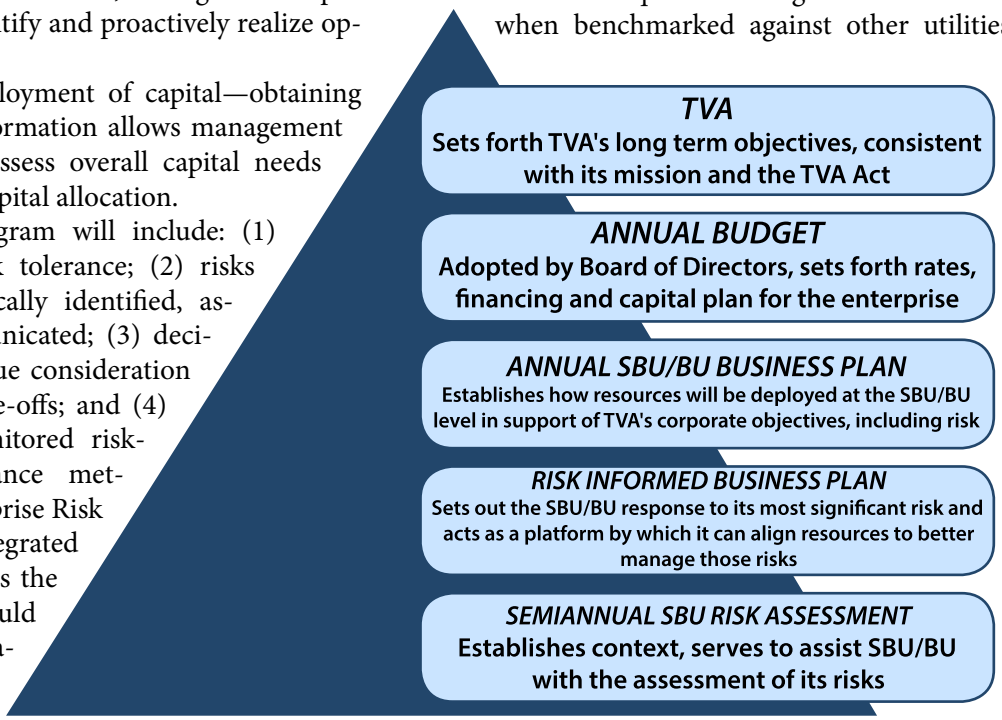
- Aligning risk appetite and strategy—management considers the entity's risk appetite in evaluating strategic alternatives, setting related objectives and developing mechanisms to manage related risks.
- Enhancing risk response decisions—enterprise risk management provides the rigor to identify and select among alternative risk responses—risk avoidance, reduction, sharing and acceptance.
- Reducing operational surprises and losses—entities gain enhanced capability to identify potential events and establish responses, reducing surprises and associated costs or losses.
- Identifying and managing multiple and cross-enterprise risks—every enterprise faces a myriad of risks affecting different parts of the organization, and enterprise risk management facilitates effective response to the interrelated impacts and integrated responses to multiple risks.
- Seizing opportunities—by considering a full range of potential events, management is positioned to identify and proactively realize opportunities.
- Improving deployment of capital—obtaining robust risk information allows management to effectively assess overall capital needs and enhance capital allocation.

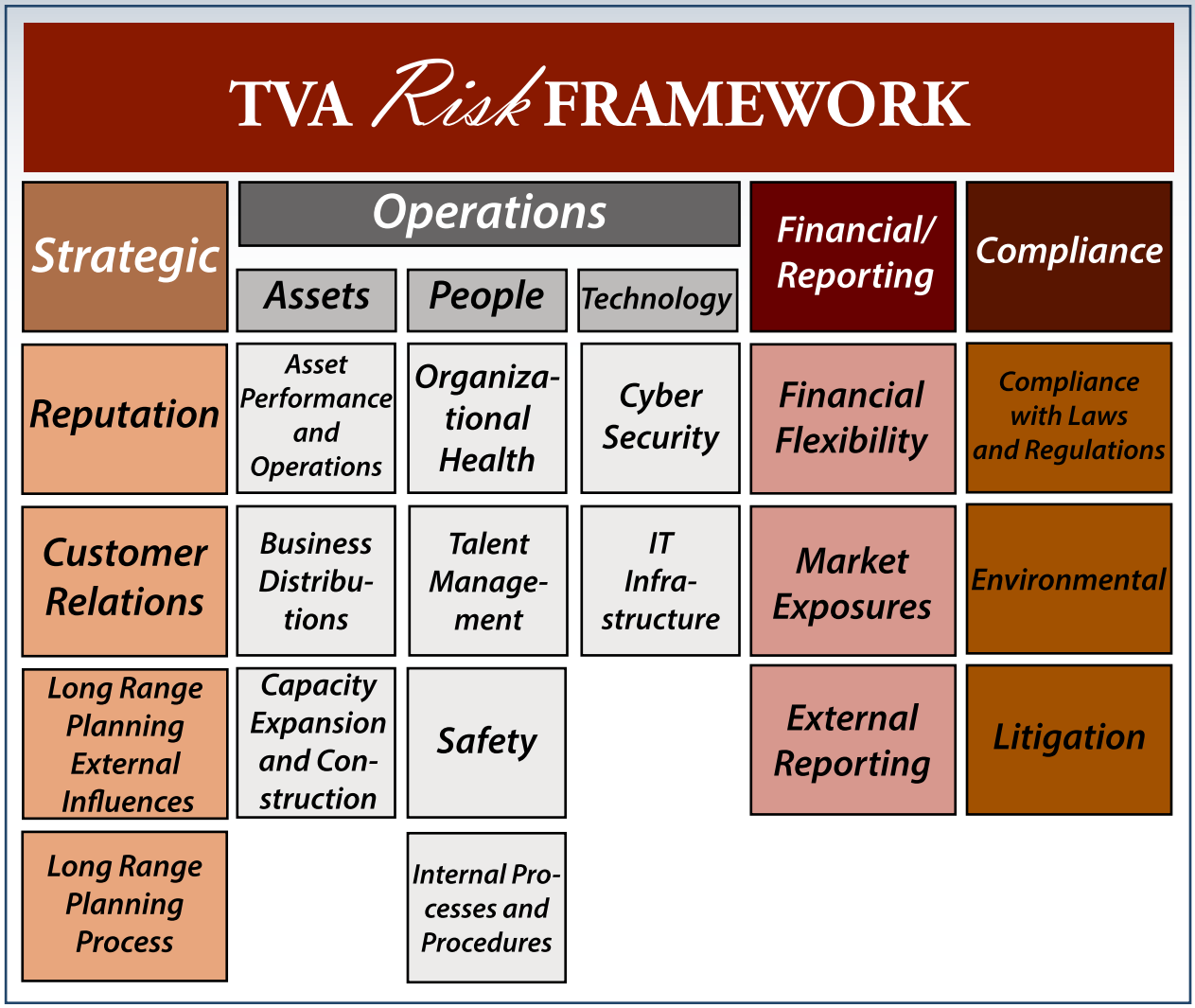
A mature program will include: (1) a well-defined risk tolerance; (2) risks that are systematically identified, assessed and communicated; (3) decisions made with due consideration to risk/return trade-offs; and (4) specified and monitored risk-adjusted performance metrics. COSO's Enterprise Risk Management Integrated Framework suggests the chief executive should assess the organization's enterprise risk management capabilities. In one approach, the chief executive brings together business unit heads and key functional staff to discuss an initial assessment of enterprise risk management capabilities and effectiveness. Whatever its form, an initial assessment should determine whether there is a need for, and how to proceed with, a broader, more in-depth evaluation.

THE TVA EXPERIENCE WITH RISK MANAGEMENT

Risk management at the Tennessee Valley Authority before the December 2008 Kingston coal ash spill was never the subject of much focus from TVA stakeholders. That environmental disaster resulted in the release of about 5.4 million cubic yards of coal ash spilling onto adjacent land and into the Emory River, more than a billion dollars in cleanup costs and litigation. After the spill, both TVA management and its stakeholders have taken a hard look at how well TVA manages risks.

TVA's evolution was probably similar to other government agencies and private sector companies through the years. That is, the design evolved; the culture did not. While the components of ERM improved significantly, the program was not supported by a healthy corporate culture. At the time of the Kingston coal ash spill, TVA ranked in the lower fourth quartile of organizational health when benchmarked against other utilities.





Among other things, this meant that confidence in TVA leadership was low, that it was safe to raise one's hand and that employees' concerns about risks would receive a fair assessment. Fortunately, the TVA board and TVA's leadership recognized the importance of improving TVA's culture after Kingston and started a process to address the culture issues.

What difference does it make to an organization's risk management program that its organizational health is improving? Employees who believe that management is demonstrating respect for their opinions and is making it safe to offer differing opinions will volunteer the discretionary effort it often takes to raise a potential risk. Employees begin to align with the vision and goals of the organization and view risks no longer as just problems for management but risks for their success as individuals. Risk identification appears now to be driven deeper into the agency and the best information about risk seems to be getting the right analysis. The ultimate success of TVA's on-going culture change, therefore, will likely have a pronounced effect on the ultimate success of its risk management program.

Currently, TVA has a chief risk officer with a staff dedicated to facilitating discussions about risk within TVA. The risks that are identified in these discussions are evaluated, and the risks are ranked with mitigation plans to reduce them as appropriate. The CEO meets periodically with the Risk Council, made up of senior executives, to review and discuss emerging risk issues. Additionally, the TVA Board of Director's Audit, Risk, and Regulation Committee routinely reviews the top ranked risks and the related mitigation efforts. The OIG serves in an advisory capacity by routinely meeting

with the chief risk officer to stay abreast of emerging risk issues.

Through time, TVA's ERM program has evolved to the point that it is now embedded in how the company conducts business, and it has progressed significantly since the Kingston spill. Particularly noteworthy is that risk management discussions occur at the plant level, and employees with direct knowledge of operations and risk identify issues. As a result, the number of risks identified has grown substantially. These risks are rolled up into 19 risk areas that are judged significant enough to impact TVA as an enterprise. (See chart on page 5.)

DEVELOPING CLARITY AROUND THE ROLE OF THE OFFICE OF INSPECTOR GENERAL IN ASSESSING AN ENTERPRISE RISK MANAGEMENT PROGRAM

The scope of responsibility for an OIG in risk management does not appear to have been the subject of much public debate. Agency risks differ significantly based upon the varied missions of federal agencies and, correspondingly, the work of IG offices differ based on the specific responsibilities of their respective agencies. All IG offices, however, regularly engage in risk assessments for their respective agencies without necessarily evaluating the ERM program specifically. As we noted above, two critical components of a robust ERM program are organizational health and the right design for the program. An examination of both would seem to be a logical part of any OIG's work. The "best in class" private sector companies seem to appreciate that organizational health and risk assessment are both key to performance or "the bottom line." Federal agencies will perform better and more likely achieve their stated goals, if like their private sector counterparts, they understand what makes a healthy culture and what is needed to have a robust ERM program.

Richard Moore

Richard W. Moore was sworn in as TVA's first presidentially-appointed inspector general May 9, 2003.

From 1985 until his confirmation as inspector general, Moore served as assistant U.S. attorney for the Southern District of Alabama. During that time, he prosecuted a variety of federal crimes including government program fraud cases, bank and insurance fraud cases, official public corruption and federal RICO cases. He also served at various times as the senior litigation counsel and as chief of the Criminal Division in the Southern District. From 1997 to 1998, Moore was an Atlantic Fellow in Public Policy at Oxford University, Oxford, England, where he conducted an independent study on the prosecution of complex international fraud cases. Prior to serving with the U.S. Attorney's Office, he was in private practice in Mobile, Ala., and Cleveland, Ohio.

Moore attended undergraduate school at Spring Hill College in Mobile, Ala., graduating summa cum laude with a Bachelor of Science degree. He graduated from the Cumberland School of Law in Birmingham, Ala., with a Juris Doctor degree.

Moore served as chair of the investigations committee of the Council of the Inspectors General on Integrity and Efficiency from May 2009 to April 2011.

Ben Wagner

Ben Wagner serves as the deputy inspector general for the Tennessee Valley Authority and is responsible for the management of the day-to-day operations of the TVA Office of Inspector General.

Prior to serving as the deputy inspector general, Wagner served as the assistant inspector general for audits and inspections and was responsible for the management of the OIG audit program. Additionally, Wagner has held other management positions in the administrative and audit operations of the OIG. Before working in the OIG, Wagner held various management and staff positions primarily in the TVA nuclear power program.


$8,000.00
$7,000.00
$6,000.00
$5,000.00
$4,000.00
$3,000.00
$2,000.00
$1,000.00
$-
1
2
3
4
5
6

The Balanced Scorecard: An Effective Performance Tool for Offices of Inspector General

By Inspector General Scott Dahl and Kathleen Frampton

In President Barack Obama's 2011 State of the Union address, he remarked, "We shouldn't just give our people a government that's more affordable. We should give them a government that's more competent and more efficient."[1] At a time of increasing fiscal austerity, all government organizations, including offices of inspectors general, must manage and improve performance to be more efficient and effective. Employing performance management systems, like the Balanced Scorecard performance management tool, can facilitate performance improvement and provide OIG managers with the necessary data to make informed decisions.

PERFORMANCE MANAGEMENT CONSISTENT WITH OIG MISSION AND VALUES HEALTH, SAFETY AND WELFARE OF MEN AND WOMEN IN UNIFORM

Much of an OIG's attention is properly focused on improving an agency's programs and operations, but an OIG also must look internally to improve its own operations and processes to deliver timely, relevant and high-impact oversight to stakeholders. To make OIG operations more efficient and effective, OIG managers need sufficient data and metrics on performance to benchmark progress and make strategic decisions about effective resource allocation.

Many OIGs develop strategic plans identifying organizational goals and objectives, establish metrics to track performance and develop specific strategic initiatives to improve processes or performance. Likewise, the Council of the Inspectors General on Integrity and Efficiency recently adopted a five-year strategic plan that incorporates specific performance measures tied to its strategic goals and objectives. The CIGIE plan identifies strategic and far-reaching objectives and targets, which CIGIE management believes are attainable and will improve CIGIE's service to its members, Congress and the public.

A familiar saying "what gets measured gets done" provides the foundation for performance management. The key to the success of performance-management initiatives is linkage of the organization's mission with a system for measuring and tracking the performance on goals and deliverables. A performance management system provides data points on how well the organization is performing in the various functional areas. It thereby plays an important role in strategic decision-making by highlighting those areas that are not performing as expected or identifying areas in need of improvement or greater management attention.

In addition, OIG managers can use the data from the performance management system to communicate with staff about how well the organization is doing on achieving its strategic objectives. The increased awareness will help to focus the staff on the highest priorities and will enhance organizational transparency and accountability. The data also can be used to make mid-course programmatic corrections during the year, making the OIG

"A familiar saying "what gets measured gets done" provides the foundation for performance management."

1) Address Before a Joint Session of the Congress on the State of the Union, 2011, Daily Comp. Pres. Doc. 1 (Jan. 25, 2011)

more flexible and adaptive to address emerging issues.

Moreover, a performance management system will assist in making the most efficient resource allocations. Almost all agency budgets have been cut and are being closely scrutinized for further reductions. OIGs are likewise experiencing corresponding budget cuts. Despite cuts, many statutory requirements for OIGs are unremitting, and in fact, in some cases, the requirements have increased. As a result, we have to do more with less. Performance management is an enabler, helping managers align resources to the highest priority projects.

THE BALANCED SCORECARD APPROACH

A performance management system widely accepted in the private sector, and more recently in government and not-for-profit organizations, is the Balanced Scorecard approach. Prior to the 1990s, business managers primarily used financial data to determine the health of a business and make strategic business decisions. Financial data generally provides a historic picture of performance, but relying solely on this backward look at performance is not optimal in making strategic decisions to drive future performance. It omits critical data about organizational performance, such as employee training and development and customer satisfaction. In the early 1990s, Robert Kaplan and David Norton

introduced the Balanced Scorecard, a strategic and operational tool linking financial and nonfinancial data to indicate organizational performance and enable better strategic decision making.[2]

Key to the BSC is the interrelationship of four perspectives on which the BSC is based: customer data, learning and growth (of employees), internal processes and financial data. Financial and customer data are historic or lagging indicators, whereas internal processes and learning and growth are forward looking, or leading indicators, and are drivers for future performance. BSC enables managers to align the vision and strategy implementation with operations by measuring performance across the four perspectives. These cause-and-effect relationships between leading and lagging indicators present a clear picture of factors affecting performance. Strategy implementation is fueled by measuring and managing mission-critical success factors

across the four BSC perspectives, which in turn leads to mission accomplishment.

In addition, the BSC is an important communication tool, providing employees and stakeholders with a clear and concise understanding of important factors to accomplish the organization's mission. Communication is critical in successfully implementing a BSC. Employees need to understand how the work they do feeds into organizational performance and strategy. The BSC provides clear linkages from work to mission accomplishment. For stakeholders (funders, appropriators and customers), a BSC demonstrates accountability and a willingness to be transparent.

An outgrowth of the internal-processes perspective and an important component of the BSC is process improvement. Process improvement drives organizational change and promotes innovation by evaluating the status quo and considering new

2) Kaplan, R.S. & Norton, D.P. (1992, January/February). The Balanced Scorecard–Measures that Drive Performance. Harvard Business Review, 70(1).

ways of doing business. By identifying those mission-critical processes and empowering employees to re-engineer those processes, breakthroughs in organizational efficiency can occur.

Overall, the BSC is a tool that provides a framework for organizations to take a holistic view of the organization to determine what progress is being made and lagging indicators. It also enables organizational leaders to identify areas that need management attention, whether to improve performance or change processes. When fully integrated into the fabric of an organization, BSC serves as a strategic management system, measurement system and communications tool.

In developing its five-year strategic plan, CIGIE used the BSC framework. Several OIGs also have used or are developing strategic plans based on the BSC framework. A helpful resource guide for developing BSC for an OIG is Paul Niven's book, "Balanced Scorecard Step-By-Step for Government and Nonprofit Agencies."[3]

APPLICATION OF THE BALANCED SCORECARD IN OFFICES OF INSPECTOR GENERAL

The OIG's mission as agency watchdog opens countless avenues for expending limited resources. OIGs must have effective systems and processes to guide work planning and better focus resources. The systems also allow us to assess our performance in meeting our organizational goals. The BSC approach dovetails neatly with OIG first principles, because it is grounded in an organization's strategic plan and core values, including accountability, performance excellence and integrity. Because oversight of the agencies for which we are responsible centers on holding these organizations accountable, to be responsible and credible, we also should hold ourselves accountable to how well we are performing against our strategic goals. We should focus on our own results and be prepared to measure our progress in achieving them to better serve our stakeholders.

Using the BSC approach, the OIG senior managers first establish the OIG's strategic goals and then identify objectives, those activities or processes that must be completed to achieve the strategic goals. OIG managers develop metrics that provide quantitative data to monitor progress towards achieving the objectives. Some objectives may cross OIG office boundaries. For example, an objective such as "timely delivery of OIG products" will encompass audit, investigation, legal analysis and congressional response metrics. This organizational view of the OIG will enable senior staff to identify areas that warranted management attention or process improvements.

As the OIG begins BSC implementation, the senior staff responsible for an objective will need to identify specific performance measures and targets. In addition, these measures can be validated and benchmarked against other OIG offices. Many measures are likely to be focused on timeliness, which is one of the primary objectives for an OIG. Measures and targets can be refined and adjusted through time to better reflect the OIG mission and strategic intent.

In addition, some objectives may involve process improvement to make the OIG a more efficient

3) Id. (2008).

and effective organization. An example of process improvement could include the audit process to improve quality, relevance and timeliness of audit reports. The outcomes of this process improvement may involve defining the audit workflow, developing a baseline measure of timeliness, reducing data calls and increasing transparency for OIG leadership. Another example of process improvement on the investigation side might be hotline processes to better standardize the intake, referral and review process, increase timeliness of complaint disposition and develop a trend analysis of complaints. The outcomes of the hotline process-improvement project include consistent communications with complainants during complaint review process, increased timeliness of complaint disposition and increased management attention to complaint trends.

A benefit of employing BSC is the ability of managers at all levels of the organization to track progress, identify risks and mitigate those risks before they have become larger problems. BSC is an excellent communication tool for providing the entire organization a data-driven picture of performance on mission goals. BSC can be posted on the OIG intranet and discussed with the staff throughout the year.

OIGs already gather, for various products, much of the data that BSC tracks, such as semiannual reports, Office of Management and Budget reports, congressional responses and others. No special software or specialized training is needed to use BSC.

"BSC is an excellent communication tool for providing the entire organization a data-driven picture of performance on mission goals."

LEGISLATIVE REQUIREMENTS FOR PERFORMANCE MANAGEMENT

BSC can also assist OIGs in meeting statutory performance management requirements. In response to presidential initiatives beginning in the 1990s, government managers have focused on becoming more results-oriented and providing more information to the public about their operations. In addition, agencies are required by the Government Performance and Results Act, and more recently the GPRA Modernization Act of 2010, to measure and monitor performance. Prior to GPRA, agency management and decision making were based on activities and processes rather than results and outcomes. A requirement of GPRAMA is that federal agencies must develop a multi-year strategic plan to identify their mission, specific goals or objectives and define performance measures or milestones that indicate progress toward goal attainment and results. GPRAMA also requires agencies to provide data about programs that cross agency boundaries and ensure quarterly data is available on public websites. To meet the requirements of GPRAMA, BSC is a tool that has a proven track record of enabling organizations to develop and implement strategic plans and to measure and track performance.

In addition, federal regulations require that agencies use a performance management system to evaluate senior executive service personnel. Performance plans must include measurable results and strategic planning initiatives. Senior executive system performance plans can be tied to BSC measures and performance on strategic initiatives, and these measures cascade throughout the OIG.

CONCLUSION

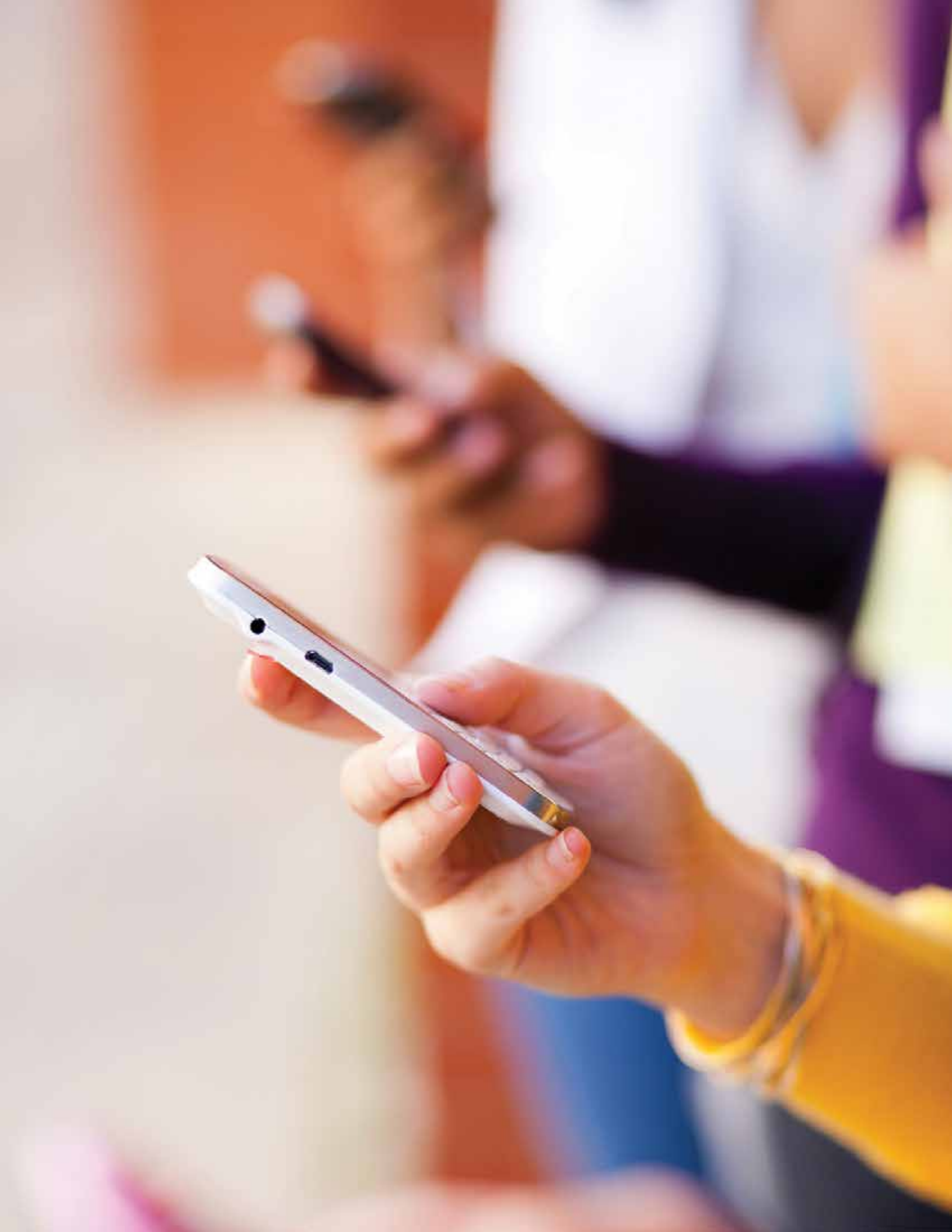
The Balanced Scorecard performance management system is a proven, flexible, inexpensive, and dynamic tool that is easily adaptable to any organization. BSC provides a straightforward framework to more effectively define the organization's priorities, make strategic decisions and evaluate performance. In addition, BSC is an excellent communications tool within the organization that provides a clear picture of its health and priorities.

Scott Dahl

Scott S. Dahl was appointed as inspector general of the Smithsonian Institution Jan. 16, 2012. Prior to his appointment, Dahl served in other senior positions in the inspector general community—first as senior counsel to the inspector general at the Department of Justice, then as deputy inspector general for the Office of the Director of National Intelligence (which oversees the Intelligence Community), and most recently as the deputy inspector general for the Department of Commerce. Before joining the IG community, Dahl was a corruption prosecutor in the Public Integrity Section, Criminal Division of the Department of Justice, and a trial attorney in the Civil Fraud Section, Civil Division of the Department of Justice. Prior to government service, Dahl was an associate at the Washington, D.C., law firm of Arnold & Porter. For the past 21 years, Dahl has been an adjunct professor at the Georgetown University Law Center, teaching classes on professional responsibility and public corruption.

Kathleen Frampton

Kathleen Welch Frampton currently serves as a business consultant in the Department of Defense. She has extensive experience in project management, performance management, process improvement, strategy development, and organizational studies and analyses. Frampton has served in the Department of Commerce Office of Inspector General, National Weather Service, Office of the Director of National Intelligence Office of Inspector General and the Department of Veteran Affairs. Prior to returning to government, Frampton was a management consultant with Touchstone Consulting Group. In addition, Frampton is adjunct faculty at the University of Maryland University College, Graduate School of Management and Technology. She is a certified project management professional and Lean Six Sigma green belt.



An Ounce of Outreach is Worth a Pound of Enforcement

By B. Chad Bungard

Advances in communications and technology have granted people real-time access to information through social networking, mobile applications and traditional Web browsers. These days, we would much rather click a mouse or swipe a touch-screen than grab a book from the shelf. This trend has had a seismic impact on American society; as a sign of the times, the Encyclopedia Britannica—an iconic publication—recently discontinued printing hard copies after more than two centuries. [1]

There were 215 million Americans actively[2] using the Internet in August 2011,[3] according to recent Nielsen Internet usage data. During that same month, Google and Yahoo! experienced 176 million and 149 million unique visitors, respectively.[4] A 2010 Pew Internet and American Life Project Report revealed, "Americans are turning in large numbers to government websites to access information and services" and "typically rely on search engines to guide them to their destination when seeking government information online."[5] According to the report, 41 percent of Americans have downloaded government forms.[6]

Scam artists are well aware of these staggering numbers. It was only a matter of time before unscrupulous individuals targeted the Social Security Administration—an agency that touches the lives of virtually every American. SSA issues a Social Security number to all U.S. citizens, permanent residents[7] and temporary working residents, and SSA benefit payments serve as the financial lifeline to many Americans.[8]

"...Americans are turning in large numbers to government websites to access information and services..."

THE NET FORMS SCHEME

In 2009 and 2010, a Google or Yahoo! search for a "new or replacement Social Security card" would likely have led consumers to the website, ssnhome.com (pictured). The site appeared at or near the top of the search results in the sponsored section of both the Google and Yahoo! search engines.

The sleek site greeted visitors with the prominent words, "Social Security Home," an eagle logo, and a subtle image of the U.S. flag at the top of the webpage. An official-sounding slogan, "Securing America's Promise," sat above two large images of a Form SS-5, SSA's Application for a Social Security Card. The site displayed many Social Security-related words and phrases, and featured "statement of earnings" and "eligibility quiz" tabs. The site offered the consumer the ability to download the SS-5 form and avoid long lines by applying from home. It also contained images of three official federal government logos: the White House, USA.gov and SSA. A click on the first two logos took the consumer directly to the official sites; the SSA logo,

1) Julie Bosman, After 244 Years, Encyclopedia Britannica Stops the Presses, The New York Times, March 13, 2012. See http://mediadecoder.blogs.nytimes.com/2012/03/13/after-244-years-encyclopaedia-britannica-stops-the-presses.
2) Nielsen Wire, August 2011—Top US Web Brands, September 30, 2011. See http://blog.nielsen.com/nielsenwire/online_mobile/august-2011-top-us-web-brands.
3) Nielsen estimates that Americans on average spent more than 30 hours on the Internet during August 2011 and visited 99 different websites. Nielsen also estimates that 275 million Americans had access to the Internet during that same period. Nielsen Wire, supra note 3.
4) Id.
5) Aaron Smith, Government Online: The Internet Gives Citizens New Paths to Government Services and Information, PEW INTERNET AND AMERICAN LIFE PROJECT, at 2, 3 (April 27, 2010). The Pew Report found that 87% of Internet users look for information or complete a transaction on a government website. See http://www.pewinternet.org/Reports/2010/Government-Online.aspx.
6) Id.
7) 42 U.S.C. § 405(c)(2)(B).
8) As of Dec. 21, 2011, 55.4 million individuals were receiving Social Security benefits. See http://www.ssa.gov/OACT/STATS/OASDIbenies.html. See also U.S. Seniors Assoc., Inc. v. SSA, 423 F.3d 397, 497 (4th Cir. 2005) ("The government has a substantial interest in protecting Social Security, as the financial lifeline of most senior Americans, and it has a strong interest in protecting Social Security recipients from deceptive mailings"). It is also important to note that SSA offers a robust Internet presence, offering comprehensive program information and publications, Social Security forms, and the ability to file for Social Security benefits online at www.socialsecurity.gov.

however, was not an operational link—leaving individuals with the impression that they were already on SSA's official site.

The problem: the website was a fake and fooled thousands of people. Net Forms, LLC, a Houston-based company, operated ssnhome.com as part of a deceptive, profit-seeking scheme by luring unsuspecting consumers into purchasing the Form SS-5. SSA provides the SS-5 at no cost on its website, accessible at www.socialsecurity.gov or www.ssa.gov, as well as at all SSA field offices and other SSA-approved locations across the country. Net Forms purchased more than a million dollars of online advertising services from Google and Yahoo! to ensure that online searches for terms related to obtaining a new or replacement Social Security card would direct potential customers to ssnhome.com. Net Forms accumulated significant revenues from its sale of the SS-5; fees reached as high as $29.99 and often unbeknownst to the consumer, the site also charged a $9.99 automatically renewable annual membership fee.

THE LAW

In 1988, to combat a rise in deceptive mailings targeting seniors, Congress enacted Section 1140 of the Social Security Act—a provision prohibiting the misuse of words, letters, symbols and emblems of SSA.[9] This provided SSA with a consumer protection tool against misleading advertising. As the Fourth Circuit Court of Appeals recognized in United Seniors Ass'n, Inc. v. SSA, "[i]n passing Section 1140, Congress sought to protect Social Security recipients from potential identity theft, from spending their Social Security benefits on organizations camouflaging as governmental entities and from endless solicitations."[10]

In particular, Section 1140 protects SSA's brand by prohibiting the use of SSA words and symbols in advertisements, solicitations or other communications in a manner that conveys the false impression that such item is approved, endorsed or authorized by SSA, or that such person has some connection with or authorization from SSA.[11] It also prohibits the fee-based reproduction, reprinting or distribution of SSA forms, applications or other publications without authorization from SSA.[12] For these prohibitions, Congress made clear that the use of a disclaimer is not a defense.[13] This was because, as noted in the legislative history, "[m]any consumers do not read, or cannot read, disclaimers[.]"[14] In 2004, Congress amended Section 1140 to also prohibit providing services for a fee that are available directly from SSA free of charge, without the use of a prominent disclaimer that the product is available free of charge by SSA.[15]

The Social Security Administration's Office of the Inspector General aggressively enforces Section 1140. The statute provides for as much as $5,000 in civil monetary penalties for each separate violation of the Social Security Act.[16] Entities are subject to a separate penalty for each time an individual visited (or viewed) a website in violation of Section 1140 or purchased an SSA form that was sold without proper authorization. The Social Security Act also provides that a penalty of as much as $25,000 may be imposed for each time a violating broadcast or telecast is viewed.[17] Penalties collected for violations of Section 1140 are deposited into SSA's Old-Age and Survivors Trust Fund.[18]

Congress initially enacted Section 1140 to combat misleading insurance marketing tactics—often referred to as "lead card" mailings.[19] This scam typically involved a lead company sending misleading solicitations to senior citizens to lure them into completing a reply card and forwarding highly sensitive personal information to the company. This lead company would market this sensitive data to insurance companies, which in turn, would solicit

9) 42 U.S.C. § 1320b-10, as implemented by 20 C.F.R. part 498.

10) 423 F.3d. 397, 399 (4th Cir. 2005).
11) 42 U.S.C. § 1320b-10, as implemented by 20 C.F.R. part 498.42 U.S.C. § 1320b-10(a)(1).
12) 42 U.S.C. § 1320b-10(a)(2)(A).
13) 42 U.S.C. § 1320b-10(a)(3).
14) H. R. Rep. No. 506, 103rd Cong., 2nd Sess., at 68 (1994).
15) Social Security Protection Act of 2004, 108 P.L. 203§ 204; 42 U.S.C. § 1320b-10(a)(4)(A).
16) 42 U.S.C. § 1320b-10(b)(1).
17) 42 U.S.C. § 1320b-10(b)(2).
18) 42 U.S.C. § 1320b-10(c)(2).
19) See generally H. R. Rep. No. 506, 103rd Cong., 2nd Sess. (1994).

"Net Forms agreed to permanently shut down its SS-5 website operation and pay a $325,000 penalty into the trust fund..."

seniors to purchase burial and other private insurance policies. Through our aggressive enforcement efforts over the years, including countless hours of investigations and litigation, these deceptive SSA-related mailings are now rare. However, as the Net Forms case illustrates, we are now confronting a new breed of misleading SSA-related advertising via the Internet.

NET FORMS: CASE RESOLUTION

Net Forms went to great lengths to shield its identity and relationship with its SS-5 website operation. Because of the covert nature in which Net Forms operated, we had concerns the company would shelter its assets from the government's reach when it became aware of the investigation. Therefore, in partnership with the U.S. Attorney's Office, Southern District of Texas, we requested and the court granted, ex parte injunctive relief prohibiting Net Forms from operating its SS-5 websites and freezing significant Net Forms assets. We reached a settlement agreement in which Net Forms agreed to permanently shut down its SS-5 website operation and pay a $325,000 penalty into the trust fund, representing a disgorgement of its net profits.

OUTREACH EFFORTS

As the Net Forms case wore on, tying up significant resources, we realized that we could not rely solely on litigation to stem the ever-increasing tide of Social Security-related Internet fraud. During the nine months investigating and litigating the Net Forms case, the number of allegations of similarly fraudulent website operations grew exponentially.

At the beginning of fiscal year 2012, the SSA OIG Office of the Counsel to the Inspector General initiated an outreach program to combat the alarming increase of Internet-based violations of Section 1140. To combat this fraud, we met with senior officials from Google, Yahoo!, Microsoft (Bing), GoDaddy, web.com, Demand Media, Discover, JPMorgan Chase, eBay/PayPal, Visa, MasterCard and American Express. Our goal was to educate these companies about Section 1140, discuss how website operators are using the Internet (and their services) to commit fraud in violation of Section 1140 and discuss ways that we could work together. This outreach effort is helping us successfully fight this fraud using a multipronged approach, which has five key elements.

ELEMENT 1: LEARN THE GAME

The outreach meetings provided us with valuable insight and knowledge of some of the key technical aspects of how individuals use legitimate business methods to lure unsuspecting customers. For example, we learned that it is a common practice to use more than one URL (or domain name) to direct traffic to a particular website. These additional URLs, referred to as display URLs, allow website operators to increase their presence in Internet searches and direct more traffic and ultimately more business to their destination URL.

ELEMENT 2: DEVELOP RELATIONSHIPS WITH KEY CONTACTS

We developed key contacts to help us gather information quickly and expedite action. Several companies have worked with us to establish mechanisms to identify the website operators quickly, halt these schemes and even prevent such activities from starting. It used to take us up to several months to discover who was operating a particular website; it can now take only hours. We have also shut down a website within just a few days of learning of its operation; this was not possible before the outreach began.

ELEMENT 3: FIND COMMON GROUND

We conveyed to each company why it was smart business to be proactive in fighting Social Security-related fraud. Working with us would not only protect the Social Security brand and protect millions of consumers, but the company's own brand was also at stake if it conducted business with fraudulent entities. Soon, after we met with one credit card company, and it created a filtering system, with our assistance, to identify websites immediately that may violate Section 1140 and that accept (or purport to accept) its credit cards as a form of payment. The company refers all websites

that it identifies through this filtering system to SSA OIG for review. This proactive method has allowed us to take immediate action to shut down upstart websites operating in violation of Section 1140. For example, we took action against two North Carolina-based sites, socialsecuritycardservice.com and social-security-card-now.com, in just a few short weeks from notification; the website operator immediately agreed to cease its violative operations.

ELEMENT 4: CHANGE THE PLAYING FIELD

Based on our outreach efforts, Google and Microsoft (which powers both its Bing and Yahoo! search engines) modified their AdWords Terms and Conditions and Ad Content and Style Guidelines polices, respectively, to protect its users from advertisements, websites and businesses that create the false impression of a connection with a governmental agency.[20] These new policies could be extremely effective in preventing individuals and entities from deceiving SSA consumers using Google's and Microsoft's advertisement services

Google also took quick action to discontinue its ongoing advertising relationships with two Internet companies—Bennett & Gray, LLC and SimpleFilings—until it was satisfied the sites were no longer acting in violation of Section 1140. Bennett & Gray of Lindon, Utah, agreed to pay a $50,000 civil monetary penalty to settle our claim that the company violated Section 1140. The company operated the websites, www.sscards.us and www.sscardapplication.com, which offered for a fee, assistance in applying for a new or replacement Social Security card. We determined that the websites' design, along with related domain names, created the false impression of a connection with SSA. Bennett & Gray voluntarily redesigned its website operation to bring it into compliance with Section 1140, and agreed to discontinue the use of the domain names www.sscards.us and www.sscardapplication.com.

Similarly, SimpleFilings agreed to discontinue the use of the domain names, gov-tax.net/ssn-card and simplefilings.gov-tax.net/ssn-card, which we deemed to be in violation of Section 1140, voluntarily made changes to its website to further clarify its services and agreed to pay an $82,000 civil monetary penalty to settle our claim that the company violated Section 1140. We received a significant number of complaints of consumer confusion caused by the use of these domain names.

"To date, our outreach efforts have stopped 18 violative Internet operations..."

ELEMENT 5: CUT OFF THE MONEY SUPPLY

Previously, we spent months investigating violative websites only to learn that they operated overseas—likely out of our reach to shut the websites down and impose Section 1140 penalties. However, by working closely with financial institutions, we have been able to effectively combat even overseas-based schemes without jurisdictional impediment. Financial institutions have moved responsibly and quickly to stop accepting funds from sites that we have deemed are operating in violation of Section 1140. Cutting off the money supply provides a quick end to the fraudulent activity; some sites have shut down within hours after financial institutions refused to process their payments

THE RESULTS

In the first few months of fiscal year 2012, through aggressive enforcement and outreach efforts, our office halted 18 Internet-based fraud schemes that we determined were operating in violation of Section 1140. One of the sites, SocialSecurityCardService.com (pictured on page 18), followed a typical blueprint of deception for SS-5 scams. These sites

20) See http://support.google.com/adwordspolicy/bin/static.py?hl=en&page=guide.cs&guide=1308243&topic=1310877&answer=1050602 and http://advertising.microsoft.com/small-business/search-advertising/ad-content-guidelines.

typically included official-looking logos and images of the U.S. flag, Social Security cards and SS-5 applications; they also often used deceptive domain names that implied a false SSA connection.

CONCLUSION

Protecting the SSA brand ultimately protects SSA consumers. Collaborating with the entities that can stop fraud in its tracks is not only cost-effective, but it can also prevent fraud from ever occurring. This public/private sector endeavor is proving to be a powerful one-two punch against Internet scams. To date, our outreach efforts have stopped 18 violative Internet operations in less time than it took to shut down the Net Forms website scheme. This kind of enforcement action quickly gets noticed; unscrupulous individuals will think twice before expending resources to set up a fraudulent operation, and legitimate businesses will ensure due diligence in complying with Section 1140. The tremendous success of our outreach program in just a short time demonstrates how an ounce of outreach is worth a pound of enforcement.

ACKNOWLEDGMENTS

The author would like to thank David Rodriguez, attorney, Office of the Counsel to the Inspector General, SSA OIG; Tracy Lynge, deputy assistant inspector general for external relations, SSA OIG; and Andrew Cannarsa, public affairs specialist, SSA OIG, for their significant efforts in the development and drafting of this article. The author would also like to thank David Rodriguez, Sandi Archibald, attorney, and Erin Justice, acting associate counsel for CMP Litigation for their creativity and innovation in uncharted territory, through their significant roles in the development and implementation of the outreach program. Mr. Rodriguez, Ms. Archibald and Ms. Justice have made a significant contribution towards protecting the public from fraud.

B. Chad Bungard

B. Chad Bungard serves as the counsel to the inspector general for the Social Security Administration, where he provides executive leadership as the chief legal advisor to the inspector general and senior staff. He is also responsible for administering the Civil Monetary Penalty Program, including the imposition of penalties and assessments, and the settlement and litigation of CMP cases. Prior to serving in this position, Bungard has held several positions. Most recently, Bungard served as the general counsel of the Merit Systems Protection Board, where he served as the chief legal advisor and chief legal representative.

Bungard received his Bachelor of Science degree cum laude from Liberty University, Juris Doctor degree from Regent University School of Law and Master of Laws degree in Law and Economics from George Mason University School of Law. He has been published in numerous legal publications, including the UCLA Entertainment Law Review, the Seton Hall Legislative Journal and the University of North Carolina First Amendment Law Review. He was also recognized as a practitioner contributor in the 9th Edition of Black's Law Dictionary.


MARKETING
SOCIAL
MEDIA
INTERNET
SEO
SHARE
INFORMATION
COMMUNITY
SEARCH
BUSINESS
CONNECTION
FORUMS

What Social Media Has to Offer Offices of Inspectors General

By Nancy Eyl

The federal government likes social media. According to the Government Accountability Office, as of April 2011, 23 of 24 major federal agencies had established accounts on Facebook, Twitter and YouTube.[1] As of June 2012, about 700 different federal departments and agencies are using more than 1,000 Twitter accounts.[2] The FBI has more than 250,000 Facebook fans, and NASA has about 2.6 million Twitter followers.[3] The General Services Administration recently launched a social media registry where government agencies can list up to 22 different social media platforms each agency uses (and constituents can check whether a site is legitimate). Twitter donated its entire archives to the Library of Congress.[4] Despite all this activity, though, a recent report, rating 34 federal executive agencies' "Klout scores" for social media impact, did not mention a single Office of Inspector General.[5] Neither did GovLoop and OhMyGov's Government Social Media Leaderboard, which has a separate category for small agencies.[6]

The Council of Inspectors General on Integrity and Efficiency New Media Working Group report points out that OIGs actively using new media are a minority.[7] Just slightly more than half (39) of the 79 CIGIE members polled responded to the survey the working group sent out. (In comparison, 67 of the 68 CIGIE members responded to an earlier CIGIE/DHS OIG hotline survey.)[8] Only two-thirds (26) of new media survey respondents identified themselves as "new media users." Appendix B of the report, which lists how OIGs use such tools as LinkedIn, Twitter, Facebook, SharePoint, RSS feeds, survey tools, WebEx, YouTube and Max, shows that most OIGs using new media largely use internal tools. Few are invested in interactive social media. The report highlights several creative uses of interactive media, including that National Archives and Records Administration OIG uses Facebook to help recover missing documents and other artifacts, and the U.S. Postal Service OIG involves the public in ongoing audits through its Audits Projects blog.[9] However, as of the survey, only one OIG used YouTube, nine OIGs used Twitter, and three used Facebook. In addition to the fact that few OIGs are using social media interactively, not all investigators, auditors and inspectors routinely use social media to collect information. It also is unlikely that most OIGs follow social media trends on the issues

"The report highlights several creative uses of interactive media, including that National Archives and Records Administration OIG uses Facebook to help recover missing documents and other artifacts..."

1) U.S. Gov't Accountability Office, GAO-11-605, Social Media: Federal Agencies Need Policies and Procedures for Managing and Protecting Information They Access and Disseminate 4–5 (2011).
2) Ines Mergel, *Working the Network: A Manager's Guide for Using Twitter in Government,* IBM Center for the Bus. of Gov't, May 14, 2012, at 10.
3) *See Government Social Media Leaderboard: How does your Agency's Social Media Presence Stack up?,* GovLoop, http://www.govloop.com/page/government-social-media-leader (last visited Aug. 1, 2012) (listing agencies according to their social media impact).
4) Matt Raymond, *How Tweet it Is! Library Acquires Entire Twitter Archive,* Library of Congress Blog (APR. 14, 2010), http://blogs.loc.gov/loc/2010/04/how-tweet-it-is-library-acquires-entire-twitter-archive/. Twitter donated its archive on April 14, 2010, the same day the Library of Congress' Twitter feed (@librarycongress) crossed 50,000 followers.
5) See Mergel, supra note 2, at 48. A "Klout Score" uses data from social networks in order to measure one's social media impact and reach. See Klout, http://www.klout.com (last visited Aug. 17, 2012).
6) *See* GovLoop, *supra* note 3.
7) U.S. Dep't of Homeland Sec. Office of Inspector Gen., Recommended Practices for Office of Inspectors General Use of New Media, OIG-11-120 (2011), *available at* http://www.ignet.gov/randp/cigienewmediarpt1111.pdf (focusing broadly on all forms of electronic, digitalized, and interactive media, not just social media).
8) U.S. Dep't of Homeland Sec. Office of Inspector Gen., Recommended Practices for Office of Inspector General Hotlines 2 (2010), available at http://www.ignet.gov/randp/ighotline1010.pdf.
9) See United States Postal Serv., http://auditprojects.uspsoig.gov/ (last visited Aug. 1, 2012).

they oversee or monitor their agency's activities and performance through social media analytics.

Two questions arise. First, why aren't more OIGs incorporating social media into regular operations? Second, how are the OIGs using social media actually using it? Are they using it to its full advantage?

In this article, I will describe some of the benefits that social media offer. Although I practice law at an OIG, I do not intend to cover social media legal issues or give legal advice.[10] Rather, I will discuss how social media can help OIGs do three things critical to the OIG mission: collect, disseminate and exchange information. I then will offer two additional reasons as to why OIGs need to be aware of social media. First, employees are using it whether an OIG does or not, and employees need guidance. Second, the Obama Administration increasingly is requiring agencies to leverage digitalized technology, and social media is a part of that. In the conclusion, I discuss factors that make it hard to justify ignoring social media. By that, I mean that the privacy, legal and information security issues are manageable; many resources already exist; and an OIG can start with less than one full-time employee. Therefore, for a relatively little investment, an OIG may get a big bang.

SOCIAL MEDIA BENEFITS

GATHERING INFORMATION

Helping Investigators, Auditors and Inspectors

Even in investigations focused on only one person, social media can help investigators find a subject's other email addresses; telephone numbers; addresses; social media monikers; hidden assets; the spoils of workplace thefts being sold on e-commerce and online auction sites; evidence of lavish purchases; travel destinations; and other facts to help establish a pre-incident and post-incident timeline. Social media can establish motives, prove and disprove alibis, and establish crime or criminal enterprise. Colleagues', neighbors' or friends' posts can provide many leads in an investigation, which a suspect's telephone records or bank account information may not show. Ranging from online dating to video sharing, social media can provide a lot of information that may be pertinent to OIG investigations for those trained to look for it. Take conspiracy, for example. Even when private communications are not readily available, just knowing who is "friends" with whom can help an investigator unravel a conspiracy to commit a crime. Social media can reveal connections by two or three degrees of separation.

"Think of social media like contemporary communication channels—if you tune in, you can hear what people are talking about."

Similarly, auditors and inspectors can use social media to gather information. Many businesses, state and local governments, and other entities have a presence on social media platforms. Contract and grant recipients, whether individuals or entities, have social media connections, as do federal government employees.[11] Auditors can explore those connections to see whether a local government official or federal contracting officer awarded a grant or contract to a family member or close connection. As with investigators, social media can help auditors identify sources of ancillary income; discover information that a person has hidden; and provide additional evidence of fraud and wrongdoing.

Tune In to Social Media to Follow News

In addition to helping investigators and auditors, social media allows an OIG to follow public conversations about mission-critical issues. Think of social media like contemporary communication channels—if you tune in, you can hear what people are talking about. Keeping abreast of public conversations and cutting-edge news can help OIG personnel address concerns promptly and effectively. Following mainstream press no longer suffices. With everyday "citizen-reporters" often breaking the news, any OIG public affairs office

10) The new CIGIE permanent standing working group for new media will, among other things, issue educational guides on legal, informational security, and privacy issues. For a brief overview of the some of the legal issues, see the CIGIE New Media Report, which outlines such legal issues as records management, privacy, procurement, terms of service, intellectual property, and ethics. Appendix D of the report lists some applicable laws and regulations.

11) Auditors should check with counsel before looking up federal employees' social media activities as part of an audit. Caveat notwithstanding, public posts are public.

seeking information about a crisis before the story hits mainstream news needs to tune into social media.

More and more government agencies are tuning in. According to a Request for Information that the FBI published in January 2012, "[s]ocial media has become a primary source of intelligence because it has become the premier first response to key events and the primal alert to possible developing situations."[12] It "trump[s] traditional first responders" including police, firefighters, EMTs and journalists. With this in mind, the FBI is conducting market research "to determine the capability of industry to provide an open source and social media alert, mapping, and analysis application solution." Among other required capabilities, solutions must provide instant notification of breaking events and emerging threats and geo-locate them onto geo-spatial maps. They also must put coding and critical infrastructural layers onto geo-spatial maps, including U.S. domestic and international terror data, and U.S. embassies, consulates and military installations worldwide. Finally, solutions must allow searching and monitoring of all publicly available tweets or postings in social networking sites.

DHS has been actively monitoring social networks for at least two years. In 2010, the DHS Office of Operations Coordination and Planning, including the National Operations Center, launched a social networking monitoring and media capability to help DHS components respond to the earthquake in Haiti and the BP oil spill, and prepare for the 2010 Winter Olympics. In February 2011, DHS published a notice regarding a new system of records, stating, "the NOC will use Internet-based platforms that provide a variety of ways to follow activity related to monitoring publicly available online forums, blogs, public websites and message boards."[13]

In addition to monitoring instant developments, an OIG also can use social media metrics to assess sentiment analysis.[14] Currently, most metrics tools focus on private-sector consumer behaviors and business metrics. A Google search for "social media audit" reaps plenty of information on how to measure a business's performance, but nothing at first glance seems tailored to the government. This is changing. On June 4, the Navy issued a solicitation that may help develop metrics tools for the public sector. This new tool will empower the Navy to monitor the conversation "surrounding" the Navy.[15] It also will allow the Navy to measure its ability "to effectively tell the Navy's story to the public," and "measure interaction (not just passive consumption)" and "advancement of key messages."[16]

DISSEMINATING INFORMATION

In addition to collecting information, OIGs can use social media to disseminate information. Doing so could serve at least three objectives: 1) help educate people about fraud, waste and abuse; 2) help increase appropriate hotline use; and 3) help OIGs control the message about the work they do (rather than allowing other organizations to speak for them). Despite some OIGs' concerns about public relations pitfalls, disseminating information for these purposes is a valid function of the OIG.

Social Media is an Educational Tool

Consider the numerous Web sources that say that social media is now the No. 1 online activity.[17] An August 2011 Pew Internet survey showed that 65 percent of adults on the Internet use social networking sites—more than double the percentage reported in 2008.[18] This represents half of all adults in the U.S.[19] Given this market share, social media presents an ideal platform for OIGs to educate the public—including federal government employees—about preventing, detecting, and reporting fraud, waste, and abuse, and to shore up confidence in

12) Social Media Application, Fed. Bureau of Investigations, Strategic Info. & Operations Ctr. (Jan. 19, 2012), https://www.fbo.gov/utils/view?id=7f9abf0ff0fdba171d1130ddf412aea3.
13) DHS/OPS—004 Publicly Available Social Media Monitoring and Situational Awareness Initiative System of Records, 76 Fed. Reg. 5603 (Feb. 1, 2011).
14) Beware of a backlash. In February 2012, at a hearing before the Committee on Homeland Security's Subcommittee on Counterterrorism and Intelligence, members of Congress criticized DHS for hiring a contractor to monitor criticism of, and public reaction to, DHS policies and response activities, and policies of other U.S. government departments and agencies. Several members expressed support for the Electronic Privacy Information Center's proposal that DHS suspend the program, claiming that this activity violates First Amendment rights.
15) *Social Media Monitoring: Solicitation No.* N00189-12-T-Z131, Dep't of the Navy, https://www.neco.navy.mil/upload/N00189/N0018912TZ13112TZ131.doc (last visited Aug. 17, 2012). The solicitation states that while the ability to track direct mentions of a given social media alias, property, or hashtag is important, the Navy is "also interested in monitoring the larger conversation that surrounds its brand and activities on a day-to-day basis." The Navy "requires the ability to track the number of times a keyword is mentioned in relation to the U.S. Navy . . . and the most popular content (measured by views and interactions) across the entire WWW mentioning the U.S. Navy (this content is not necessarily produced by the Navy, but relates to the Navy)."
16) Id.
17) I am unable to verify this statistic, but for what it is worth some sources say that social networking reaches 82% of the world's online population, or 1.2 billion users. *See, e.g., It's a Social World: Top 10 Need-to-Knows About Social Networking and Where It's Headed,* ComScore, 4 (Dec. 21, 2011), http://www.comscore.com/Press_Events/Presentations_Whitepapers/2011/it_is_a_social_world_top_10_need-to-knows_about_social_networking.
18) Mary Madden & Kathryn Zickuhr, *65% of Online Adults Use Social Networking Sites,* Pew Internet & Am. Life Project (Aug. 26, 2011), http://pewinternet.org/Reports/2011/Social-Networking-Sites.aspx.. The findings come from national survey findings from a poll conducted on landline and cell phones, in English and Spanish, between April 26 and May 22, 2011, among 2,277 adults (age 18 and older). Id. at 4.
19) *Id.* at 2.

the government through transparency and accessibility. Several OIGs use their websites to educate the public about spotting and preventing Medicaid, mortgage, tax relief, and other types of fraud. With social media, however, OIGs can reach a broader and growing audience. As social media overtakes the Web, relying solely on a website to educate people may not suffice.

Social Media May Help Increase Appropriate Hotline Use

Second, using social media to disseminate information about the OIG mission and hotline may increase appropriate hotline use. A 2010 CIGIE/DHS OIG hotline report points out that some OIGs receive more than 50,000 hotline calls a year, and many are "frivolous, misdirected, or otherwise unsuitable for further action by the OIG, creating a strain on a hotline's often limited resources."[20] Since most hotline complaints do not justify action by the OIG,[21] potential complainants need to be educated on the role and authority of the OIG. Furthermore, according to the CIGIE report, several OIGs do not provide a mechanism for reporting waste, fraud and abuse, in violation of the IG Act.[22] In addition, some do not respond to complainants or track calls, leaving people to wonder whether OIGs are listening.

The CIGIE hotline report recommends that OIG hotlines "aggressively advertise the OIG hotline to agency employees and the general public."[23] Recommendation No. 9 states that "OIG hotlines should consider engaging in education and outreach efforts to raise the profile of their hotline and its purpose to the parent organization's employees and contractors, thereby increasing the number of relevant and actionable complaints the hotline receives."[24] The report also recommends that OIGs consider evaluating technology and consider using social networking sites to facilitate hotline reporting because many individuals choose to report via Internet instead of the phone, and they probably would report via such social networking sites as Facebook, MySpace and Twitter.[25]

Using social networks to facilitate appropriate hotline reporting is working for at least one OIG. During fiscal year 2012, the U.S. Postal Service OIG referred to its Office of Investigations more than 710 leads originating from posts to its Facebook, Twitter and blog accounts.[26]

SOCIAL MEDIA MAY HELP OIGS CONTROL THE MESSAGE

As Ines Mergel writes in a newly released report, Twitter can be used to control and direct messages to influencers in the network.[27] To what extent do OIGs effectively use such social media tools as Twitter to relay the OIG story? As the GSA scandal on conference spending unraveled, how many people had never heard of GSA OIG? Despite regular mention of OIGs in the news, stating "I work for an OIG" draws blank stares at dinner parties—even in Washington, D.C. To non-feds, the federal government can appear to be an inpenetrable monolith, with little to no accountability. This can be changed if OIGs tell their own story. Moreover, if OIGs do not tell their story, others will.

Organizations such as Electronic Privacy Information Center, the Electronic Frontier Foundation, and the Project on Government Oversight are using social media to reach people and share their respective missions. POGO—the self-proclaimed "only organization focused on the inspector general vacancies"—has a "Where are the Watchdogs" page that tracks how long inspector general posts have been vacant.[28] Its podcast, "Without Inspectors General, What Government Waste Are We Missing?" discusses "how the GSA got busted." But unlike most OIGs, POGO

20. U.S. Dep't of Homeland Sec. Office of Inspector Gen., *supra* note 8, at 3.
21. *Id.* at 13.
22) *Id.*
23) *Id.* at 11.
24) *Id.* at 14.
25) *Id.* at 28.
26) Tara Linne, the U.S. Postal Service OIG's social media director, shared this story.
27) Mergel, *supra* note 2, at 19.
28) As of Sept. 6, 2012, this page lists eight IG vacancies ranging from 223 days (Securities and Exchange Commission) to 1695 days (Department of State). See http://www.pogo.org/resources/good-government/go-igi-20120208-where-are-all-the-watchdogs-inspector-general-vacancies1.html.

connects with the public via at least seven different social media outlets: Twitter, Facebook, YouTube, Flikr, podcasts, RSS feeds and a blog. According to POGO's social media director, many people who find POGO through POGO's Facebook page say that they did not know there was an organization devoted to exposing fraud and corruption in the government. Although OIGs are not competing for an audience, it is sad to think that (1) people may not know what an OIG is or (2) if they know about the OIG, they may nonetheless prefer to report fraud, waste and abuse to POGO.

Controlling the message is important because OIG interests are not always aligned with the interests of other organizations. For example, Electronic Frontier Foundation publishes "When the Government Comes Knocking, Who Has Your Back?" which rates ISPs, email providers and social networking sites based on the extent to which they publicly commit to telling users when the government seeks data about them, unless accompanied by a court order or prohibited by law.[29] EFF expects such companies to go to court to fight for their users' privacy interests and report on how often they provide data to the government. EFF reports on whether companies have joined the "Digital Due Process Coalition," a group advocating for electronic privacy legislation requiring the government to show a court-ordered warrant to access to any electronic information.[30] In addition, EFF lobbies Congress to oppose mandatory ISP and telecom data retention legislation.[31] It recently announced a "moment to celebrate" when a child protection bill passed without a data retention provision.[32]

OIG Concerns About Public Relations May Be Based on Misunderstanding

Despite the benefits of using social media to disseminate information, there are some perceived barriers. The CIGIE New Media Working Group survey results showed that some OIGs are concerned about using social media for "public relations" because such use could make an OIG appear self-aggrandizing. This concern may be based on a misunderstanding. Using social media is not about emphasizing the importance of the OIG or an OIG official. Neither is it about "puffery" or "self-aggrandizement."[33] Rather, it is about education and transparency—and leveraging technology to maximize fraud prevention. OIGs would not use social media to engage in such forbidden activities as advocating for legislation or pay raises, or encouraging the public to contact Congress regarding legislation. On the contrary, they would educate the public about what OIGs are and what they do.

Appropriations restrictions on publicity and propaganda do not prohibit an agency's legitimate informational activities.[34] In fact, the executive branch has a duty to inform the public regarding government policies.[35] Traditionally, officials have used government resources in explanation and defense of their policies—even in the absence of specific direction or a mandate.[36] GAO has consistently held that public officials may report on the activities and programs of their agencies, may justify those policies to the public, and may rebut attacks on those policies.[37]

In addition, some CIGIE survey respondents stated that directly engaging the public might exceed the OIG mission since the IG Act only requires OIGs to keep Congress and the head of the agency informed about problems and deficiencies. The IG Act does not require informing "taxpayers" or "public at large." While that is true, all U.S. government agencies serve the taxpayer, and OIGs are no exception. If taxpayers do not know the OIG exists, how can they appreciate an OIG's service? One could argue that the public needs to educate

29) *See* Elec. Frontier Found. press release (May 31, 2012), https://www.eff.org/press/releases/when-government-comes-knocking-who-has-your-back.
30) *Id.*
31) *See* Rainey Reitman, *How Internet Companies Would Be Forced to Spy on You Under H.R. 1981,* Elec. Frontier Found. (Feb. 23, 2012) (equating legislation requiring ISPs to keep electronic data for 12 months to government spying), https://www.eff.org/deeplinks/2012/02/how-internet-companies-would-be-forced-spy-you-under-hr-1981.
32) *See* Rainey Reitman, *A Moment to Celebrate: No Data Retention Mandate in Smith's New Child Protection Bill,* Elec. Frontier Found. (July 5, 2012), https://www.eff.org/deeplinks/2012/07/moment-celebrate-no-data-retention-mandate-smith%E2%80%99s-new-child-protection-bill.
33) In the past 50 years, GAO has noted that one of the main targets of the publicity or propaganda prohibition is when the "obvious purpose is 'self-aggrandizement' or 'puffery.'" See, e.g., U.S. Gov't Accountability Office, Office of the Gen. Counsel, B-284226.2, Application for Anti-Lobbying Restrictions to HUD Report Losing Ground (2000); U.S. Gov't Accountability Office, Office of the Gen. Counsel, B-302504, Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (2004). GAO has defined self-aggrandizement as "publicity of a nature tending to emphasize the importance of the agency or activity in question." U.S. Gov't Accountability Office, B-212069, Restriction Violations on the Use of Appropriations in a Press Release by the Office of Personal Management (1983) (quoting 31 Comp. Gen. 311 (1952)), [GAO's] first decision interpreting the publicity or propaganda prohibition). For example, an agency would be prohibited from using appropriated funds to issue a press release intending to persuade the public as to the importance of a government agency. *Id.* (finding OPM press releases informing the public of the Administration's position on pending legislation unobjectionable).
34) Benjamin S. Rosenthal, House of Representatives, B-184648, 1975 WL 9457 (Comp. Gen. Dec. 3, 1975) (discussing an agency's "legitimate interest in communicating with the public").
35) Medicare Prescription Drug, Improvement, and Modernization Act of 2003, B-302504, 2004 WL 523435 (Comp. Gen. Mar. 10, 2004) (citing B-130961, Oct. 26, 1972) (stating that "agencies have a general responsibility, even in the absence of specific direction, to inform the public of the agency's policies").
36) *Id.*
37) Id. (citing B-223098, Oct. 10, 1986) (stating that "public officials may report on the activities and programs of their agencies, may justify those policies to the public, and may rebut attacks on those policies").

itself—and could start by clicking on the agency website link to the OIG. But the public increasingly expects the government and other sources to share information and news directly via social media. Using social media to publicize reports could help educate the public about OIGs and help OIGs become more accessible, transparent, and participatory – as good government is envisioned.

EXCHANGING INFORMATION

In addition to collecting and disseminating information, OIGs can use social media to exchange information. Specifically, rather than just passively informing taxpayers about how to report fraud or corruption, or tweeting to Congress about a newly released report, OIGs can use social media to hold a digitalized "town hall." One IG recently used a Twitter hashtag, #AsktheIG, to collect questions from an audience of about 2,600 conference attendees.[38] By connecting to various outlets, such as email, Twitter, and LinkedIn, the IG addressed dozens of questions in real-time. Other federal government agencies do the same. In January 2012, the Department of State's daily press briefings opened questions to Twitter users tweeting to hashtag #AskState. The same month, the president hosted his first "Hangout on Google+," a group video-chat service. More than 227,000 people submitted topics for discussion. The White House also has held Facebook and Twitter town hall meetings. Using social media like this shores up public confidence.

Social media offers other opportunities to collaborate. For instance, in April 2012 the Agency for International Development announced the Tech Challenge on Atrocity Prevention, a contest seeking technological solutions to improve the ability to model or forecast the potential for mass atrocities and "link early warning to early responses."[39] In May 2011, the Navy launched a computer game, energyMMOWGLI—or Massive Multiplayer Online Wargame Leveraging the Internet—to tap players' ideas on how the Navy can meet energy needs. According to a Challenge.gov program administrator, since September 2010, 46 agencies and bureaus have published challenges, offering prizes or recognition for top solutions to problems. Receiving 300,000 visits a month, Challenge.gov is a public-engagement-oriented division under GSA's Office of Citizen Services and Innovative Technologies. To participate, all OIGs need to do is get an account, draft some specifications of a problem to be solved and then publish it.[40]

OTHER REASONS WHY OIGS NEED TO BE AWARE OF SOCIAL MEDIA

Besides the above-mentioned benefits, there are at least two additional reasons as to why OIGs need to be aware of social media: OIG employees need guidance on how to appropriately use social media so as to avoid conflicts with work-related responsibilities, and the U.S. Administration is increasingly requiring executive branch agencies to leverage technology.

Employees Use Social Media

First, OIG employees are using social media whether an OIG does or not, and employees need guidance. Drafting internal guidance may be a good idea because employees not only may use social media to talk about their home lives, but also to discuss bosses, colleagues and other aspects of their work. Employees untrained in social media may cause serious and unintended consequences, including compromised trials, impeached witnesses, cybersecurity issues and personnel problems. The story of the "Officer Who Posted Too Much on MySpace" could frighten any law enforcement agency into drafting a policy.[41] In interviews, law enforcement officers whose posts impeached them said if they had known that social media could be discoverable, they would not have posted "that stupid comment." But they posted before their employer had a social media policy, and they did not know their private social media account activities could be used by defense counsel in court. A policy will put employees on notice that social media is not the place for water cooler or locker room bravado talk. Everything in social media exists in perpetuity, and

38) Roberta Baskin with HHS OIG shared this story about IG Daniel Levinson.
39) *USAID's Tech Challenge on Atrocity Prevention,* USAID (Apr. 23, 2012), http://transition.usaid.gov/press/factsheets/2012/fs120423.html.
40) Another possibility is to seek an in-house solution. FEMA, for example, designed a mobile app that allows users to access a checklist of disaster supplies, checking what is already in the pantry so that users know what to buy. It includes an emergency contact page and the user's emergency plan – with information stored on the device and not with the agency (to address privacy concerns). The response part of the app allows users to find shelters and disaster recovery centers.
41) *See* Jim Dwyer, *The Officer Who Posted Too Much on MySpace*, N.Y. TIMES, March 10, 2009. Dwyer interviewed an officer whose MySpace posts allowed someone to beat a felony weapons charge at State Supreme Court, Brooklyn. The arresting officer posted before the trial that he was feeling "devious" and was "watching 'Training Day' to brush up on proper police procedure." *Id.*

it may be discoverable.[42] In addition, not everything is protected by the First Amendment.

"...OIG employees are using social media whether an OIG does or not, and employees need guidance."

In the private sector, there is a growing body of case law on disputes between employers and employees regarding employees' private social media activities. The Federal Trade Commission and the National Labor Relations Board, for example, are bringing complaints against companies arising from their social media activities and employee-related activity.[43] Recent cases before the NLRB show that social media policies risk violating the rights of employees as defined by Section 7 of the National Labor Relations Act, as amended, particularly when they are so broad as to restrict or chill protected activities and employee-related activity. Private employers who fire or punish employees using social media to discuss such topics as work conditions, terms and conditions of employment, managers, and management may be ordered to rehire such employees and provide back pay.

Social media has become such a "hot topic" at the NLRB since August 2011 that the NLRB's acting general counsel has issued three reports on the latest social media decisions.[44] Practitioners following NLRB case law advise employers not just to draft a policy, but to draft a policy that can be enforced. Although the NLRB and FTC do not have jurisdiction over the federal government, being familiar with the issues is important.

The U.S. Administration Increasingly Requires Agencies to Use Digitalized Technology

Second, leveraging technology is increasingly becoming an executive agency requirement. The sooner an OIG invests in social media, the easier—and arguably more efficient—it will be to implement future mandates. President Obama's most recent digital government mandate requires agencies to take even more steps towards modernizing the way they do business: On May 23, 2012, the president signed Building a 21st Century Digital Government to ensure that federal agencies use emerging technologies to serve the public as effectively as possible. On the same day, the federal chief information officer released a corresponding strategy, Digital Government: Building a 21st Century Platform to Better Serve the American People (Digital Government Strategy), outlining actions that agencies must take within one year and requiring them to post a progress report on their websites by Aug. 23, 2012. This new strategy complements several other initiatives involving technological innovation to increase efficiency, maximize interagency sharing and provide better services to the public. These initiatives include Executive Order 13571 (Streamlining Service Delivery and Improving Customer Service); Executive Order 13576 (Delivering an Efficient, Effective, and Accountable Government); OMB Memorandum M-10-06 (Open Government Directive), and the 25-Point Implementation Plan to Reform Federal Information Technology Management (25-Point Implementation Plan) (December 9, 2010).

The Administration's drive to move the government into the future—"more nimble, more cost effective and more citizen-focused," according to the 25-Point Implementation Plan—reinforces the OIG mission. Serving the public is integral to the mission of every government agency, and this is also true of OIGs. As government watchdogs, OIGs serve the public by creating a channel for complaints about fraud, waste and abuse, and by investigating wrongdoing in government. The digital initiatives emphasize reducing waste and redundancy; breaking down programmatic and agency silos to achieve more efficiency; increasing transparency;

42) *See, e.g., Trail v. Lesko,* 2010 WL 2864004, No. GD-10-017249 (Allegheny C.P. July 3, 2012) (holding that before a requesting party will be granted unfettered "access" to a Facebook account, the party must show a "sufficient likelihood" that the non-public postings would contain information that is relevant to the litigation that is "not otherwise available"). The analysis in *Trail v. Lesko* varies from the standard threshold relevancy model adopted by some courts and utilizes a balancing approach based on the "level of intrusiveness." The bulk of this 20-page opinion serves as an introduction to the discoverability of private social media content in Pennsylvania and other jurisdictions.

43) In 2009, the FTC established endorsement guidelines on what employees can say online about their company's products and services. See FTC Guides Concerning Use of Endorsements and Testimonials in Advertising, 16 C.F.R. Part 255 (2009). A company can be held liable if its employees are less than honest, and a consumer relies on an employee's comments to his or her detriment. However, since companies cannot monitor everything that employees say, those with a social media policy can take advantage of a "safe harbor" offered by the FTC in connection with its amended guidelines.

44) *Report of the Acting General Counsel Concerning Social Media Cases: OM 11-74,* NLRB (Aug. 18, 2011); *Report of the Acting General Counsel Concerning Social Media Cases: OM* 12-31, NLRB (Jan. 24, 2012); *Report of the Acting General Counsel Concerning Social Media Cases: OM* 12-59 NLRB (May 30, 2012). In the preface to the second report, the Acting IG states that social media is a "hot topic."

and pushing agencies to implement creative solutions to persistent—and costly—bureaucratic problems. For example, the Digital Government Strategy and the Federal Information Technology Shared Services Strategy (May 2, 2012) (action item No. 6 in the 25-Point Implementation Plan), stress "innovating with less." Given resource constraints, mission requirements, customer expectations, and rapidly-changing technology, "innovating with less" sounds like an efficiency-minded policy that an OIG could endorse. Similarly, the OIG mission aligns with the Open Government Initiative, which aims to create a government more collaborative, transparent and participatory.

CONCLUSION

In conclusion, social media offers many benefits to OIGs. No matter the types of programs and operations an OIG oversees, OIG staff increasingly needs social media to gather information. OIGs also can leverage social media to fulfill other functions, such as staying informed about mission-critical issues, educating the public about the OIG mission and hotline, and facilitating interactive communication. Social media can help OIGs become even more efficient and effective in their operations.

So, what is holding some OIGs back? If social media offered all of the benefits outlined above but presented unreasonable barriers, then jumping into social media would be unadvisable. But that is not the case. Several factors make it hard to justify ignoring social media.

First, as the CIGIE New Media Report points out, the legal, privacy and information security issues are manageable.

Second, many resources already exist. To cite some examples, OMB and the Chief Information Officers Council have released several guiding documents to help agencies grasp some legal and security issues associated with social media. The Howto.gov website, managed by GSA and the Federal Web Managers Council, provides sample policies and guidance on federal Web requirements and policies; cloud computing; applications; data and Web infrastructure tools; and online citizen engagement. The Web Content Managers Forum, a network of 3,000 government Web professionals from federal, state, and local agencies, maintains a professional networking space on OMB Max and holds monthly conference calls. The CIGIE New Media Report appendices include an information security primer, as well as a list of legal resources and OIGs that agreed to be contacted about their experiences with social media tools.

In addition to these resources, plenty of training is available for such disciplines as law, public relations, investigations, audits and information security. GSA, for instance, supports the DigitalGov University, which provides such training as the annual Government Web and New Media Conference.[45] In January 2012, the Washington, D.C., chapter of the Association of Certified Fraud Examiners offered five continuing professional education credits for "Social Media and Implications to the Fraud Examiner Community," covering the current social media landscape, program and policy issues, and investigative techniques. As for legal training, private organizations and local bars offer training on how to use social media tools, how to write a social media policy, etc.

Third, although agency social media activities require input and expertise from multiple disciplines, an OIG can build a social media program with one full-time employee or less. And if one full-time employee is not possible, what about sharing a contractor with another OIG or two, drafting an Economy Act agreement, or hiring an intern? That would be a start. Even more interesting and creative, perhaps, are the OIGs that are rethinking the kinds of talent they need. For instance, Craig Goscha, the Chief Information Officer for the Department of Agriculture OIG, created a new career path in his information technology shop when he replaced a departing manager with a "new media coordinator." This new IT position will involve coordinating and designing all social media platforms, keeping track of social media developments, measuring performance of social media efforts, and following forums, blogs and other outlets to keep abreast of the issues the agency is interested in. Goscha said, "It's hard to take an IT person who is trained to design and implement networks, infrastructure and security and ask them to go design code, and publish a website."

Much can be achieved even without a budget. The go-to guide for government on how to procure cloud services, for example, was done without authority or

45) Unfortunately, the conference scheduled for May 16-17, 2012, was postponed this year as "part of an ongoing top-to-bottom review of GSA's operations, including all conference spending." See Matthew Weigelt, GSA postpones conference as part of 'top to bottom review', Fed. Computer Week (May 11, 2012), http://fcw.com/articles/2012/05/11/new-media-conference-postponed. GSA also sent an email to those who registered for the conference.

a budget. In collaboration with the Chief Acquisition Officers Council and the Chief Information Officers Council, the Federal Cloud Compliance Committee published "Creating Effective Cloud Computing Contracts for the Federal Government: Best Practices for Acquiring IT as a Service," in February 2012. Since the committee's first meeting in March 2011 in the basement of the Department of Housing and Urban Development, about eighty people have joined subcommittees to work on contract clauses. Spanning across agencies and disciplines (Freedom of Information Act, records, privacy, cyber security, procurement and legal), the committee holds meetings with borrowed space and uses SharePoint to store documents.[46]

The OIG community has similar passion to make ideas happen.[47] The CIGIE New Media Working Group started with an idea and grew into a permanent standing working group. Fifteen OIGs sent representatives to regular meetings at DHS OIG from December 2010 until September 2011 to support the first phase of the work.[48] Continuing under the auspices of the CIGIE Homeland Security Roundtable, the permanent standing working group began meeting again in the fall of 2012 and soon will be publishing a detailed educational guide on legal, privacy and information security issues.[49] Meanwhile, OIG public affairs officials—"inspired" by the working group, according to one steering committee member—created their own CIGIE council and listserv.[50] Initiatives such as these show that OIG leadership and staff, like others in the government, appreciate what social media has to offer.

Nancy Eyl

Nancy Eyl is assistant counsel to the inspector general at the Department of Homeland Security. In 2011, she led interagency Office of Inspector General working group meetings on new media under the auspices of the Council of the Inspectors General on Integrity and Efficiency and was the principal drafter of the CIGIE report, "Recommended Practices for Office of Inspectors General Use of New Media" (September 2011). She currently is co-chairing the CIGIE permanent standing working group meetings.

Eyl began her legal career at the Special Inspector General for Iraq Reconstruction. Since becoming an OIG attorney, Eyl has participated on OIG panels for the American Bar Association, the Washington Foreign Law Society, and the Association of Certified Fraud Examiners. She also has provided training to the OIG and ethics communities. Most recently, in September 2012, Eyl taught the Fourth Amendment update at the IG Criminal Investigator Academy. In December 2011, the Council of Counsels to the Inspectors General recognized Eyl for outstanding contributions to the inspector general community.

Before becoming an attorney, Eyl taught Russian at Indiana University Bloomington and Russian, German and the literary genre of autobiography at Tulane University. As an academic, she received numerous awards, fellowships and scholarships, including a Fulbright to Ukraine, an award for outstanding achievement by Harvard University's Ukrainian Summer Institute, and grants supporting independent research in Germany, Ukraine and Eastern Europe.

Eyl holds a Juris Doctor degree from Georgetown University Law Center and is a member of the Supreme Court and New York State bars. Created without a mandate a few years ago, the CIGIE New Media Working Group grew into a permanent standing working group.

46) Jodi Cramer (Air Force) shared this history.
47) Based on my experience with the Council of Counsels to Inspectors General, I believe that the OIG legal community must be one of the most interactive of all government attorney associations. Among many CCIG initiatives, a noteworthy one is the wiki on OMB Max, created by Sabrina Segal (Counsel to the IG at the International Trade Commission).
48) A special thanks to CIGIE New Media Working Group members for their hard work, good humor, and passion. They are Raman Santra (DOC OIG); Gary Sternberg (EPA OIG); Roberta Baskin, Steven Hernandez, Janna Raudenbush, and Elise Stein (HHS OIG); Richard N. Reback, Louise McGlathery, Jennifer Kim, and Rene Lee (DHS OIG); Colleen Kane (HUD OIG); Sabrina Segal (ITC OIG); Tim Cross (NSF OIG); Mario Jimenez (ED OIG); Renee Juhans and Frank Mazurek (NASA OIG); Epin Christensen (Smithsonian OIG); Sonya Zacker (PBGC); Jonathan Lasher (SSA OIG); David Barnes, Alexis Buckhannon, and Karen Kraushaar (TIGTA); Tara Linne (USPS OIG); and Joanne Moffett (VA OIG).
49) As chair of the CIGIE Homeland Security Roundtable, Acting DHS IG Charles K. Edwards has continued to lead the next phase. Yvonne Manino and I are co-chairing the group. Members of the legal subgroup include Athena Jones (HUD OIG); Sonya Khanzode (NSF OIG); Steve Begg (USPS OIG); Jon Lasher (SSA OIG); Alexis Turner (TIGTA); Scott Levine (EPA OIG); Joanne Howard (USDA OIG); and Michael Boehman and Preethi Nand (DOD OIG). Members of the information security subgroup include Patrick Kelly and Steven Hernandez (HHS OIG); Jaime Vargas (DOD OIG); Stacey Lyon and Brandon Williamson (DOD OIG); Matthew Bunko and Theodore Dykstra (DOI OIG); and Magali Khalko (LSC OIG).
50) The new public affairs council is being led by public affairs officials from HHS OIG, DOD OIG, SSA OIG and TIGTA.

Law in the Shadows

By Michael Davidson and Neal Swartz

Members of the inspector general community have been involved in undercover operations either under their own investigative authority, as part of a joint operation with other law enforcement agencies or in an oversight role reviewing the activities of their parent agency. In a recent Semiannual Report to Congress, for example, the Department of Defense IG reported that the Defense Criminal Investigative Service had taken part in 16 undercover operations, partnering with Immigration and Customs Enforcement, the FBI, the Department of Commerce and the Naval Criminal Investigative Service.[1] Similarly, the Office of Treasury Inspector General for Tax Administration recently issued a publicly available report concerning Internal Revenue Service undercover operations.[2] Further, many agencies pay for information and evidence using such vehicles as confidential informants and rewards.

Despite the covert nature of these operations, there have been a significant number of legal opinions rendered concerning the application of appropriations and contract laws in the context of undercover operations and the purchase of information and evidence. As a rule, both the courts and various governmental bodies have afforded agencies an extraordinary amount of leeway. Federal criminal investigators, investigative staff and counsel, working as a team, may take advantage of significant legal tools afforded to them through the innovative use of various principles of appropriations and procurement law, including broad legal interpretations of what is considered a necessary expense of an operation when a federal investigative agency acts in an undercover capacity. Unfortunately, there has been no scholarly treatment of this topic and little guidance is publicly available to the Office of Inspectors General community concerning application of appropriations and procurement law in an undercover context. This article endeavors to partially fill that gap by discussing some of the issues commonly arising in this area.

RETAINING MONEY AND THE MISCELLANEOUS RECEIPTS STATUTE

One reoccurring issue in undercover operations is the agency's authority to retain money that it receives during such operations. Generally, all money received by or for the United States, regardless of source, must be returned to the Treasury Department. This requirement is codified in the Miscellaneous Receipts Statute, 31 U.S.C. § 3302(b), which provides that: "An official or agent of the government receiving money for the government from any source shall deposit the money in the Treasury as soon as practicable without deduction for any charge or claim."

The MRS mandate does not apply, however, when specific statutory authority exists for an agency to retain money. Several agencies possess specific statutory authority to keep and use proceeds

1) Inspector General, U.S. Department of Defense, Semiannual Report to the Congress, Oct. 1, 2010-March 31, 2011, at 53.
2) TIGTA, Criminal Investigation Can Take Steps to Strengthen Oversight of its Undercover Operations (Feb. 3, 2012).

from undercover operations, including the FBI, the Drug Enforcement Administration, the Bureau of Alcohol, Tobacco, Firearms and Explosives, ICE, and the IRS.[3]

Additionally, in at least one case, the Government Accountability Office determined that money received during an undercover operation was not the type of money falling within the scope of the MRS. In Family Lines Rail System-Return of Funds, B-20590 (Comp. Gen. May 19, 1982), a railroad company assisting an FBI undercover operation investigating theft of diesel fuel, provided fuel to the FBI with the understanding that at the end of the investigation any unused fuel or money generated from sale of the fuel would be returned to the railroad. After the sale of fuel, the FBI initially retained the proceeds of sale as evidence, but wished to return the money to the railroad at the end of the investigation. GAO reviewed the language of the MRS' predecessor statute, 31 U.S.C. § 484, and concluded that the funds were not the type of money contemplated by the statute. Although there are differences between the wording of sections 484 and 3302(b), the GAO continues to cite this decision for the position that "this is not the kind of receipt contemplated by 31 U.S.C. § 3302(b)."[4]

"When the primary (or sole) benefit of the operation resides heavily with a single law enforcement agency, that entity may still obtain the services of other agencies through reimbursable agreements."

Absent statutory authority to retain money, agencies involved in undercover operations must generally deposit money received during these operations into the Treasury as miscellaneous receipts, but strict temporal application of the MRS may be impractical. In Requirement to Deposit Receipts from IRS Undercover Operations into the Treasury, B-229631, 67 (Comp. Gen. 353, 354 March 23, 1988), for example, GAO recognized that "requiring deposits of money accrued during an undercover operation," such as gambling winnings or money generated by undercover businesses, "as soon as it is received may be impracticable within the meaning of [the MRS] in that it may jeopardize the success of the investigation." GAO determined that the IRS could treat short-term operations as a single transaction for MRS purposes.

JOINT OPERATIONS

As noted in the opening paragraph, agencies oftentimes engage in joint operations. This may reduce operational costs, and it allows for the sharing of information, expertise, assets and equipment. Unfortunately, GAO has provided little guidance about joint funding of law enforcement operations.[5] Assuming the normal rules of obligation and expenditure apply, each participating agency must satisfy the basic fiscal limitations (purpose, time, and amount) of its own appropriations to participate in the joint operation.

In addition, each participating agency should be able to contribute proportionally to the operation considering the benefit to each agency without improperly augmenting the appropriations of another participating agency. Further, no prohibition appears to exist on the contribution to the mutually-benefiting operation being a combination of funds, equipment or investigative assets.

When the primary (or sole) benefit of the operation resides heavily with a single law enforcement agency, that entity may still obtain the services of

3) U.S. General Accountability Office, II Principles of Federal Appropriations Law 6-213 n.185 (3rd ed. January 2004) [hereafter GAO Red Book].
4) GAO Red Book, at 6-182.
5) See generally Interagency Funding, 15 GAO-RB pt A, s.3, 2008 WL 6969351 (G.A.O., September 2008, March 2011 Update).

other agencies through reimbursable agreements. For example, it is well established that one agency may obtain the services of an employee of another agency through a reimbursable detail under the authority of the Economy Act.[6] Indeed, the Economy Act provides broad authority for one agency to purchase services (and goods) from another.[7]

INSURANCE

The government follows a policy of insuring its own risk of loss or damage to government property and for the liability of government employees under circumstances when the United States is responsible for their actions (e.g., tort claims). Accordingly, in the absence of express statutory authorization, an agency may not use appropriated funds to "purchase insurance to cover loss or damage to government property or the liability of government employees."[8] However, on at least one occasion, GAO determined the normal prohibition against insurance purchase did not apply and such purchases were necessary expenses of the agency, when the agency involved in an undercover operation required insurance to maintain the cover of an undercover proprietary business.

In FBI Insurance From Private Firms In Undercover Operations, B-204486 (Comp. Gen. Jan. 19, 1982), GAO determined the FBI could purchase insurance during its undercover operations if the agency determined such expenses were necessary for the success of the operation or to protect the safety of its undercover agents. GAO noted the FBI was not seeking to purchase insurance to protect itself from financial loss, which would run afoul of the self-insurance policy, but rather the FBI believed purchase of insurance was necessary to maintain the cover of its front corporations, facilitating their appearance as a normal business enterprise.[9] In the event of an accident, auto insurance may be a prudent investment to avoid having to go overt with local law enforcement entities, private counsel for injured parties and insurance companies. Absent private insurance, any claims for injuries or property damage caused by an undercover agent would likely be treated as a claim under the Federal Tort Claims Act, 28 U.S.C. §§ 1346(b), 2671-2680.

6) Inspector Gen., Library of Congress, B-247348, 1992 WL 152986, at *9 n.3 (Comp. Gen. June 22, 1992).
7) 31 U.S.C. § 1535(a).
8) GAO Red Book, at 4-176.
9) Id. at 2.

LOSING MONEY

GAO has been very forgiving when an agency loses control of funds during an undercover operation. Agents may need large amounts of cash to establish their credibility with the object of an investigation. Frequently referred to as a "flash roll," the money may be used to purchase drugs, counterfeit currency or products, illegal firearms or other types of contraband, or as a gambling stake.

"GAO determined the FBI could purchase insurance during its undercover operations if the agency determined such expenses were necessary for the success of the operation or to protect the safety of its undercover agents."

In some circumstances, an agent advanced cash for use in an operation may be held accountable for its loss. Generally, if the money is lost under circumstances considered an inherent risk of the operation, such as a suspect fleeing with the money or robbing the agent, the agent will not be held accountable for the loss, and the money will simply be charged against the financing appropriation as a necessary expense of the operation. If the agent's negligence is responsible for the loss, however, he/she may be held accountable.[10] For example, in Mr. Paul R. Gentile, financial manager, Bureau of Alcohol, Tobacco and Firearms, B-232253 (Comp. Gen. Aug. 12, 1988), an ATF agent advanced $900 to a confidential informant to rent an apartment as part of an undercover operation. Instead, the CI fled with the rent money. Because the agent was not negligent, GAO determined that the loss could simply be treated as an operating expense. In contrast, in Carole J. Dineen, fiscal assistant secretary, Department of the Treasury, B-214718 64 (Comp. Gen. 140 Dec. 14, 1984), GAO denied relief to a Secret Service agent, whose shoulder bag was sto-

10) Funds To Which Accountability Attaches, 9 GAO-RB pt. B, s.3(a)(2), 2006 WL 6179214, at *3-4 (G.A.O., February 2006; March 2011 update).

len containing $1,000 to be used to purchase counterfeit U.S. currency. While in a crowded airport in Columbia, the agent put his bag on a counter to make travel arrangements and then noticed after approximately five minutes that the bag was gone. GAO determined that the agent had been careless with the funds and his negligence was responsible for the loss.

PURCHASING INFORMATION AND EVIDENCE

The concept of investigative agencies using appropriated funds to purchase evidence and information from confidential informants has been a firmly rooted principle of appropriations law since at least 1951. The comptroller general held that the former Customs Services could fund the purchase of information and evidence from its appropriation available for the Customs Services' law enforcement activities without requiring a specific appropriation for rewards as long as such expenditures were "administratively determined necessary in the enforcement of the customs . . . and narcotics laws." See The Honorable Secretary of the Treasury, B-106230 (Comp. Gen. Nov. 30, 1951) (reviewing the law enforcement appropriations of the Customs Service and the IRS). The general rule that emerges is that the use of appropriations for payments for information concerning violations of those laws administered by an agency is generally considered a necessary expense of the appropriations that are available for the enforcement of those same laws. See e.g., Cash Prize Drawing by National Oceanic and Atmospheric Administration, 70 Comp. Gen. 720, 721-22 (1991). For most agencies involved in undercover operations or other law enforcement operations, there are multiple funding sources for the purchase of information and/or evidence. Some agencies receive annual appropriations that include money specifically intended for the payment of information. Congress, however, oftentimes places a cap within an agency's appropriations act on the amount of such funds available for this purpose. Where an agency receives an appropriation providing for the purchase of information or evidence, but where that appropriation is capped, an interesting question arises about whether any specific purchase of evidence falls within that limited appropriation or whether the investigative agency's necessary expense authority (e.g., B-106230) controls. Such a question normally will be resolved by reference to which appropriation is more specific for the expense in question.

Agencies with statutory authority to retain proceeds generated during an operation (aka churned funds) also may possess the authority to use such funds to purchase information and evidence as a necessary operational expense. In addition, both the Department of Justice Asset Forfeiture Fund, 28 U.S.C. § 524(c), and the Treasury Asset Forfeiture Fund, 31 U.S.C. § 9703, may serve as a funding source to purchase information.

Agencies may be authorized to spend appropriated funds on rewards to informants or other sources of information through specific statutory grants of authority. Agencies with specific statutory authority to pay rewards include the Department of State, 22 U.S.C. § 2708, the Secret Service, 18 U.S.C. § 3056, the IRS, 26 U.S.C. § 7623, the Department of Justice, 18 U.S.C. §§ 3071-72 and 28 U.S.C. § 530C(b)(1)(L), the Postal Service, 39 U.S.C. § 404(a)(7), and ICE using the former Customs Service's moiety authority, 19 U.S.C. § 1619.

If an agency lacks specific statutory authority to pay rewards, then it may only do so "if the information is 'essential or necessary' to the effective administration and enforcement of the laws" (administered by that agency) and the reward money comes from an appropriate funding source, considering the agency's organic authority and the language of its appropriations act. Information that is merely "helpful or desirable" does not justify reward money.[11]

In Internal Revenue Service "Informant/Witness" Expenditures, B-183922 (Comp. Gen. Aug. 5, 1975), GAO determined that the IRS' general ap-

11) GAO Redbook at 4-276 - 278.

propriation was available to support and maintain an informant/witness as a necessary expense of its investigation until such time as a more specific appropriation became applicable (i.e., DOJ Witness protection Program). As discussed below, there have been a surprising number of cases seeking rewards or enhanced rewards by informants.

INFORMANT LAWSUITS SEEKING COMPENSATION FROM THE GOVERNMENT

A surprisingly large number of cases exist discussing attempts to sue the United States, seeking compensation for information or services provided to law enforcement agents. The bulk of the cases are brought under the Tucker Act, relying on either an implied-in-fact theory of recovery or alleging a violation of a money-mandating law or regulation.

The Tucker Act provides jurisdiction to the U.S. Court of Federal Claims to "render judgment upon any claim against the United States founded . . . upon any express or implied contract with the United States." 28 U.S.C. § 1491(a)(1). If the amount of money sought is less than $10,000, a federal district court also has jurisdiction. 28 U.S.C. § 1346(a)(2).

However, establishing Tucker Act jurisdiction by itself is insufficient to obtain damages from the United States. The Tucker Act is only a waiver of sovereign immunity that allows a court to hear and decide a case; it does not provide a substantive right to damages against the United States. To obtain damages, the plaintiff must either establish a breach of an express or implied contract with the United States, or bring a claim based on the violation of a law or regulation that mandates compensation for its violation.

In most cases brought on an express or implied-in-fact contract theory, informants frequently lose because the field agents who allegedly promised money for information or cooperation lacked the authority to bind the United States contractually. To illustrate, in Roy v. United States, 38 Fed. Cl. 184 (Fed. Cl. 1997), a confidential informant, who agreed to work for the FBI in a highly successful bookmaking/money laundering sting operation targeting drug rings in the Philadelphia area, received a significant sentence reduction as well as more than $180,000 in compensation. Subsequently, Roy filed suit seeking as much as 25 percent of all money and assets seized because of his contributions to the sting operation, basing his entitlement on an alleged oral contract with FBI special agents

"However, establishing Tucker Act jurisdiction by itself is insufficient to obtain damages from the United States."

Treating the lawsuit as one brought under the Tucker Act, the court noted that Roy had to establish the traditional elements of a contract—mutual intent to be bound, offer, acceptance and consideration—as well as the actual authority of a government representative to bind the United States contractually. The court determined that the FBI agents lacked any actual authority to create an enforceable contract with an informant, that supervisory agents who may have possessed such authority never exercised it and that the special agents lacked "implied" actual authority because contracting authority was not an integral part of FBI agents' duties, even when working with confidential informants. When an agent or other law enforcement official is authorized to contract with an informant, however, the courts will enforce the terms of any such agreement. See Forman v. United States, 61 Fed. Cl. 665 (2004)

In addition, there has been quite a bit of litigation in cases involving rewards, particularly cases involving the IRS reward program. A key issue in these cases has been whether the terms of an alleged contract, in particular the amount of reward, are too ambiguous to be enforceable.

In Golding v. United States, 98 Fed. Cl. 470 (2011), an informant unsuccessfully alleged that the U.S. Postal Service breached an implied-in-fact contract for a reward to pay for information and services provided during a government investigation. Postal Service posters offered rewards for certain amounts, based on specific offenses, "for information and services leading to the arrest and conviction of any person for the . . . offenses." Further, the posters stated, "The amount of any reward will be based on the significance of services rendered, character of the offender, risks and hazards involved, time spent and expenses incurred."

"...the government may also be required to notify the informant that any eventual moiety award may be offset by prior payments for information of evidence."

Reviewing analogous IRS reward cases, the court opined that for the complaint to survive a motion to dismiss, plaintiff had to allege that the agency somehow fixed the amount for the reward or agreed to pay a specific sum. The terms of the alleged contract, the court determined, did not "mandate an award in every instance" and were "too indefinite for contract formation unless and until specific reward amounts are negotiated and fixed with appropriate, government officials."[12]

The courts have also addressed attempts to sue the United States for compensation based on a violation of a money-mandating law or regulation. For example, courts have determined that Moiety 19 U.S.C. § 1619, is money mandating, but the statute creating DOJ's Asset Forfeiture Fund, 28 U.S.C.524(c)(1)(B), and the Reward statute, 18 U.S.C. § 3071, are not. Perri v. United States, 340 F.3d 1337 (Fed. Cir. 2003) (DOJ Asset Forfeiture, moeity); Fleming v. United States, 413 F. Supp.2d 503 (E.D. Pa. 2005) (Reward statute).

The moiety statute provides that the secretary of the treasury, now DHS, may pay an award to any person, not a federal employee, who (1) detects, seizes and reports the seizure of certain items subject to seizure and forfeiture under customs or navigation laws or (2) furnishes original information to a U.S. Attorney, the secretary of the treasury or a customs officer concerning "fraud upon customs revenue" or a violation of customs or navigation laws; that results in a recovery of duties withheld, fines, penalties or forfeited property. 19 U.S.C. § 1619(a). The secretary may also provide an award to any otherwise eligible person when the forfeited property is not sold, but instead is destroyed or given to a government agency for official use.[13]

Significantly, the regulations implementing that statute require the customs officer receiving information to notify the informant "that, in the event of a recovery, he may be entitled to compensation." 19 C.F.R. § 161.14. Depending upon the specific agreement between the government and informant, the government may also be required to notify the informant that any eventual moiety award may be offset by prior payments for information of evidence.[14]

Despite permissive statutory language stating the secretary "may" pay an award, in Doe v. United States, 100 F.3d 1576, 1582 (Fed. Cir. 1996), the U.S. Court of Appeals for the Federal Circuit examined the legislative history of the statute and held that it mandated payment of some amount of an award when the statutory conditions for award eligibility were met. To recover under the moiety statute, however, a plaintiff must also establish the statutory prerequisites to recovery: that he/she "provided original information involving violations of the customs or navigation laws that has led to the recovery of a fine, penalty or property." In addition, the government enjoys great discretion in determining the amount of award, as much as 25 percent per case of any related recovery or unsold forfeited property. 19 U.S.C. §§ 1619(a),(b),(c).

CONCLUSION

Some federal investigative agencies have specific statutory authority excepting their undercover operations from legal principles that, while necessary for normal agency operations, interfere with the practical needs of an undercover investigative capacity. Even without specific statutory authority, most investigative agencies may take advantage of expansive legal interpretations of what is a "necessary" expense of an agency appropriation when maintaining the covert nature of an operation, developing and protecting a source or gathering information and evidence. The authority to retain money earned in investigative operations and the authority to purchase insurance, for example, allow a federal investigative team to look and act like a private sector enterprise. Further, the authority to purchase necessary information and evidence through advertised rewards is often crucial to obtaining information to investigate a crime. Finally, the ability of investigative agents to develop and pay informants without obligating the government

12) d. at 484.
13) Id. § 1619(b).
14) Id.

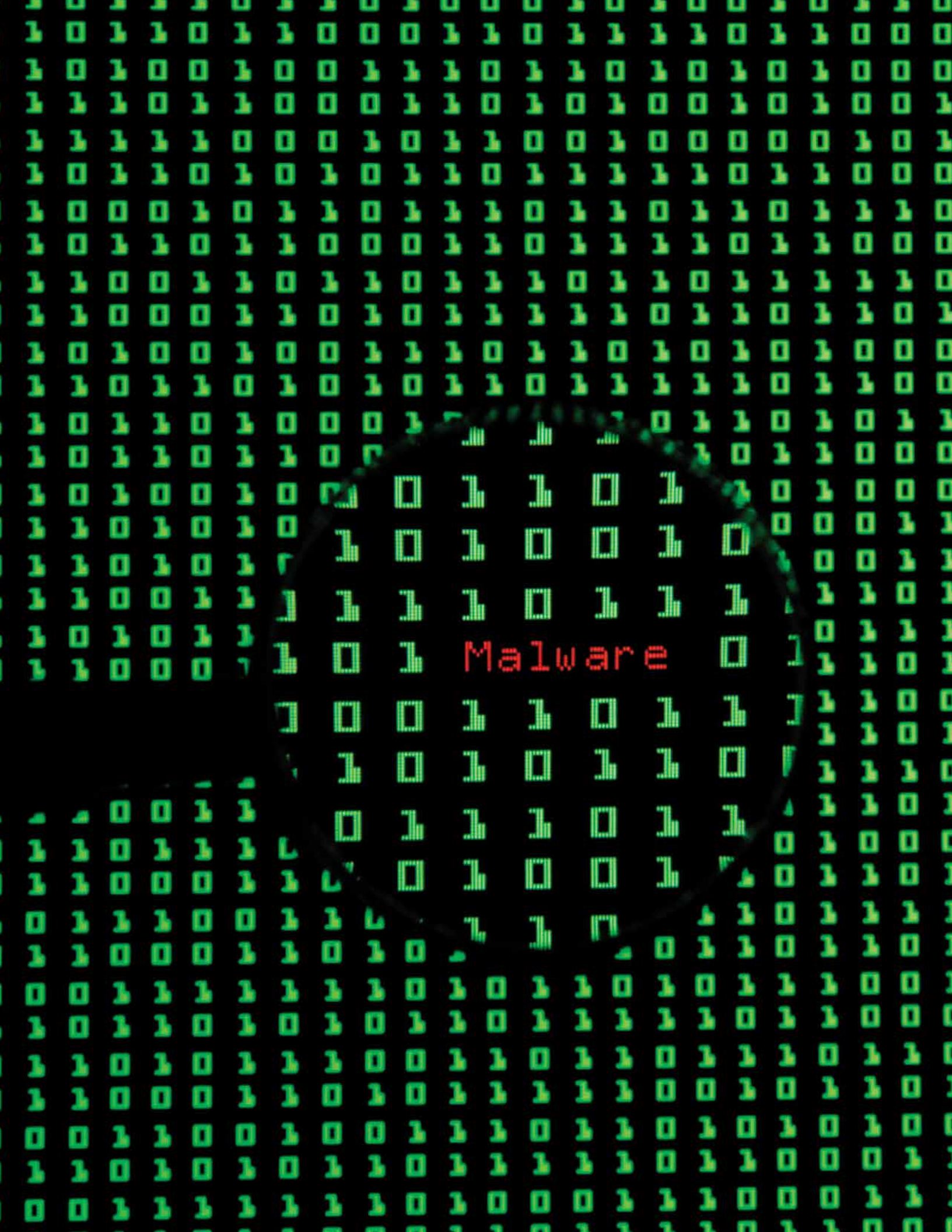
contractually advances the needs of an investigation while protecting an agency's funding from future spurious claims. As investigators, advisors or when acting in an oversight role, the OIG community should be familiar with these legal authorities. ☙

Neal Swartz

Neal J. Swartz has been the chief of the Commercial and Administrative Law Division of the Immigration and Customs Enforcement, Office of the Principal Legal Advisor since November, 2007, and has practiced appropriations, procurement and grant law in various positions for the Department of Homeland Security and the Department of Justice. Mr. Swartz earned his Juris Doctor from the Columbus School of Law at the Catholic University of America and his Bachelor of Arts from the University of Notre Dame.

Michael Davidson

Michael J. Davidson is a supervisory contract and fiscal law attorney with the Office of the Principal Legal Advisor, Immigration and Customs Enforcement. He has previously served as a litigation and supervisory attorney with the Department of the Treasury. He also practiced law as an Army judge advocate, retiring from the Army after twenty-one years of service. His prior assignments have included branch chief with the Army Procurement Fraud Division, as a special assistant U.S. attorney in Arizona specializing in procurement fraud and public integrity prosecutions and as a special trial attorney with Department of Justice's Civil Fraud Section. Davidson earned his Bachelor of Science degree from the United States Military Academy, his Juris Doctor from the College of William & Mary, a LL.M. in Military Law from the Army's Judge Advocate General's School, a second LL.M. in government procurement law from George Washington University, and a Doctor of Juridical Science in Government Procurement Law from GWU. His doctoral dissertation focused on procurement fraud.


Malware

Botnet Investigations: An Inspector General Perspective

By Sean Zadig

Deep within the heart of the agency, late at night after the employees have all gone home, desktop and laptop computers awaken and begin to work. All across the country, in agency offices and employee homes, these computers begin to process data and execute commands. But instead of performing tasks for the workers who usually tap at their keyboards, the computers are serving a different master, half a world away. They have been forced to join a botnet (robot network), and are stealing sensitive data, conducting attacks on other computers and are enriching their new masters, all without the knowledge of the agency's users or information technology staff. In fact, the infected computers are now under the complete control of the bot masters and can perform their every bidding.

While it may sound like a plot to a zombie horror movie, millions of computer systems worldwide have been infected with malicious software (malware), have been enslaved into botnets—including computer systems owned and operated by the U.S. government—and are under the control of criminals. Vint Cerf, one of the original inventors of the Internet, estimated that perhaps one in four computers on the Internet are a part of a botnet,[1] indicating they are extremely pervasive. This new menace provides fresh challenges to inspector general cybercrime investigators who seek to keep their agencies free from computer-based criminal activity. This article will describe the types of botnets in modern use and how IGs are uniquely qualified to investigate these crimes, and it will discuss a current example as a case study.

TYPES OF BOTNETS

There are many different varieties of botnets in use today, each with their own criminal purposes and unique threats to agency systems. The table below, adapted from the author's previous work ,[2] provides a typology that will guide the discussion in this article. As we will see, most botnets are created and maintained for financial gain, in that they exist to

FIGURE 1. COMMON BOTNET TYPES

Botnet Type	Purpose	Example Botnet
Spam Information stealing	Delivering unsolicited e-mail Stealing login credentials to banks and websites, or intercepting credit card numbers	Storm Worm Zeus
DDoS	Denial of service attacks against websites or servers	BlackEnergy
Dropper Intelligence gathering, cyberwarfare Click fraud	Installing other types of malware Allegedly state-sponsored surveillance or destruction to further political means Fraudulent clicks upon online advertisements	Bredolab Ghostnet, StuxNet
Other	Illegal web hosting, proxies	Bahama, DNSChanger Avalanche, Koobface

1) Tim Weber, "Criminals 'may overwhelm the Web,'" *BBC News.* January 25, 2007, accessed Oct. 3, 2010, http://news.bbc.co.uk/2/hi/business/6298641.stm.

2) Sean M. Zadig and Gurvirender Tejay, "Emerging cybercrime trends: Legal, ethical, and practical issues." In Investigating cyber law and cyber ethics: Issues, impacts, and practices, ed. Alfreda Dudley, James Braman, and Giovanni Vincenti, (Hershey, PA: IGI Global).

enrich the criminals by abusing the computing and network resources of the infected systems. Unfortunately, the malware for many of these botnets can be purchased in underground forums, are sold as "kits" and often come with technical support from their developers, making the barrier to entry for aspiring bot masters relatively low.

The oldest types of botnets are those that exist to send spam, and botnets are responsible for the majority of the spam that ends up in inboxes today.[3] One infected computer can send spam to thousands of recipients in a single day. Spam can be a profitable enterprise for the bot masters and is used for a number of illegal purposes to promote products, such as counterfeit pharmaceuticals and counterfeit designer goods; to send email lures, (also known as "phishing" emails), that ask recipients to enter their email account or bank account credentials for future use by criminals; and to engage in stock market manipulation by pumping penny stocks that are later dumped at a profit or to simply spread other viruses and malware by enticing recipients to click on fraudulent links or open tainted documents, thereby infecting themselves. Spam botnets in themselves do not pose great risk to agency systems; however, they can be a foothold for other types of malware, and IT staffers expend considerable resources remediating infected computer systems.

"Government agencies have come under frequent attack in recent years as part of demonstrations linked to the hacker movement known as Anonymous..."

A different type of botnet that does have more inherent risk to government computers is the malware associated with "information stealing" botnets. Computers infected with this type of malware essentially act as miniature wiretaps and intercept victims' keystrokes and capture documents. When

users type sensitive information on their keyboards, such as login credentials to agency systems or passwords to banks or financial systems, the information is sent to the bot masters, who can use it as they please. More advanced malware, including one botnet generally referred to as "Zeus," can even use the infected victim computers as a proxy to remotely access bank accounts and quickly wire out the contents. The impact upon government systems is clear: intercepted login credentials may allow criminals unfettered access to sensitive emails and documents, and agency employees can suffer great personal losses if their identities are stolen or bank accounts robbed. In fact, the Zeus malware has previously drained bank accounts associated with local governments, clearly demonstrating the willingness and adaptability of the criminals to monetize their illicit accesses where possible.

Another common type of botnet malware is associated with distributed-denial-of-service attacks. This malware turns each infected bot into what can be thought of as a digital missile that can be aimed at other computers, websites or networks on the Internet, and when many bots attack a single target, they can quickly overwhelm it with requests and knock it offline. Distributed-denial-of-service attacks can affect government agencies in two ways: the agency's computers can be used to execute the attack if they are already compromised and are part of a botnet; or the agency may itself be a target of an attack. Government agencies have come under frequent attack in recent years as part of demonstrations linked to the hacker movement known as Anonymous, although distributed-denial-of-service attacks are also regularly executed for illicit financial reasons. For example, small businesses are often extorted with threats of attacks—a very real

3) Jim Carr, "TRACE: Six botnets generate 85 percent of spam." *SC Magazine,* March 4, 2008, accessed Oct. 15, 2010, http://www.scmagazineus.com/trace-six-botnets-generate-85-percent-of-spam/article/107603/.

threat to companies that depend upon the Internet for their livelihood. One common distributed-denial-of-service botnet malware kit is known as "BlackEnergy" and can be purchased for as little as $40 on underground forums.[4]

Yet another type of botnet is often referred to as "loader" or "dropper" malware, and it exists purely to install other types of malware for a price. The bot masters can build up botnets of thousands of infected computers, and subsequently charging other cybercriminals to install malware so they can build their own botnets. This has given rise to an underground economy, known as "pay per install," where infected computers can be bought and sold cheaply. Budding bot masters need only pay another criminal to do the hard work of infecting the computers for them and can then select the computers that will be a part of the new botnet. For example, the bot master may want to join government systems to an information stealing or intelligence gathering botnet or may enlist computers with fast Internet connections to distributed-denial-of-service or spam botnets. The threat of this type of malware to agency systems is clear, as espionage-minded criminals or nation-state actors could also purchase infected computers in this underground market for nefarious uses.

This leads into the next type of botnet—intelligence gathering or cyberwarfare. A malware network known as "Ghostnet," believed by industry experts to have originated in China, was recently found on computer systems in embassies and governments around the world. Based on press reporting, the "Stuxnet" botnet was also associated with attacks on nuclear facilities in Iran. While law enforcement options in the face of state-sponsored botnets can be limited, investigators need to be aware of this type of botnet, as it may become more prevalent in the future.

Online advertising is a multibillion-dollar industry and provides much of the revenue that powers popular online services such as Google, Facebook and others. Consequently, a type of botnet that is becoming more and more common is associated with an activity known as "click fraud," a type of fraudulent activity designed to subvert the online advertising industry. It often operates on a "pay-per click" model; each click on an advertisement from a website visitor results in a small payment to an advertiser. Infected computers in the botnet are often made to click on advertisements under the control of bot masters, often by hijacking the websites that the victims intended to visit, thereby inflating the advertising accounts with fraudulent clicks. The impact to agency computers with this type of botnet is similar to those associated with spam botnets—while the click fraud operations may not impact agency operations directly, this type of malware can be expensive to remediate, and as the agency computers are under the control of organized cybercriminals, may introduce other types of malware onto government networks. A recent click fraud investigation will be used as a case study later in this article.

There are a number of other types of botnets in existence. For example, the "Avalanche" botnet was used to host bank phishing websites and was responsible for two-thirds of all phishing attacks in 2009.[5] Other types of botnets turn victim computers into a proxy network, allowing cybercriminals to disguise their online location and conduct online criminal activity in relative safety by appearing to originate from the infected computer. In reality, bot masters are limited only by their imaginations and their desire to make money, and undoubtedly, new types of botnets will come into existence.

IG INVESTIGATIONS OF BOTNETS

Armed with a basic understanding of the types of botnets, we turn our attention to the investigation of these threats. Agency OIGs are, in fact, well suited to investigate this type of criminal activity for a number of reasons. Unlike investigative agencies, such as the FBI or Secret Service, with cybercrime

4) Jose Nazario, "BlackEnergy distributed-denial-of-service bot analysis," October 2007, Arbor Networks technical report.

5) Greg Aaron, "The state of phishing," *Computer Fraud & Security,* Vol. 2010(6), pp. 5-8.

missions, OIGs have a number of advantages in these cases. First and foremost because corporate victims are often hesitant to report attacks for fear of bad publicity and the FBI may need to wait for an individual or organization to contact them to report a botnet infection, the victimized agency is in a better position to clearly assess and characterize losses. Moreover, the OIG's mission and authorities provide a clear basis for action when warranted.

The Inspector General Act of 1978 ("the Act") provides many of the basic tools needed to conduct these investigations. The Act insures that IG investigators will have access to agency records, which include IT security incident records documenting the malware infections, network logs and copies of infected computers as evidence, and other information that can be used to calculate the cost to the agency of the attack. Agency computers are considered protected systems under Title 18 U.S.C. § 1030, and intrusions and damages into protected systems are punishable as felonies, with recent changes to the statute specifically criminalizing botnet activity.

The IG also has administrative subpoena power under the Act, a tool that other cybercrime investigative agencies do not possess. Subpoenas are indispensable tools when conducting botnet investigations and can be used in many different ways. They can be used to request the identity of criminals who purchased online domain names or rented computer servers that are used to control the botnet or install the malware. They can also be used to seek subscriber information for email accounts associated with those domain names and servers, which may then lead to social networking accounts and other means of identifying targets. Equally important, administrative subpoenas can be used to follow money trails—in the case of click fraud botnet investigations, for instance, subpoenas can identify who was receiving the illicit proceeds from hijacked clicks.

IG subpoenas also offer significant benefits when compared to grand jury subpoenas. Agents do not need to convince a prosecutor to open a case to get subpoenas through the grand jury—this allows IG investigators time to fully develop a case and to make it more appealing if the case is eventually presented to an assistant U.S. attorney. Additionally, with no secrecy requirements imposed by the grand jury, agents can more easily work with other agencies, most notably foreign counterparts, or with subject matter experts to investigate the case.

"The NASA OIG examined agency IT security records and determined that more than a hundred NASA computers had been infected..."

Depending upon the size and geographic distribution of the botnet infections within the agency, there may be a number of venues from which to choose. If infected computers are located throughout the country, or if money trails lead to a particular locality in the U.S., agents may opt to bring the case to a prosecutor with experience or interest in investigating botnets. This runs in contrast to agencies such as the FBI or SS, which often have to work exclusively with their local U.S. attorney's office, whether or not the USAO's priorities or resources align adequately with the novelty and complexity of a botnet investigation. And investigators should also consider coordinating with other OIG offices; after all, if one agency is affected by a particular botnet, there is a good chance that other agencies are as well. Such coordination between OIGs can pay dividends later on, for issues such as selecting venue for prosecution, more accurately assessing and reporting overall damage amounts from the malware attacks and uncovering additional investigative leads.

A CASE STUDY: THE DNSCHANGER BOTNET

The botnet known as "DNSChanger" is an example of an IG-driven botnet investigation. This investigation has not been fully adjudicated, so only a brief overview will be presented.

In late 2009, the NASA OIG and the FBI opened a joint criminal investigation into the activities of a company known as Rove Digital, which according to security experts was the source of a click fraud botnet known as DNSChanger. This botnet allowed the subjects to surreptitiously direct millions of victims to websites of the subject's choosing, instead of the websites that the victims intended to visit. In the case of more than one hundred NASA computers, the malware forced the computers to use Rove Digital's DNS servers instead of NASA's DNS serv-

ers, which placed them into a sort of a botnet under the control of Rove Digital.

The NASA OIG examined agency IT security records and determined that more than a hundred NASA computers had been infected by servers under the control of Rove Digital for losses exceeding $65,000. Forensic examinations of a number of these computers, as well as analysis of network logs, confirmed they had their DNS settings changed via malware. Using a combination of IG subpoenas and grand jury subpoenas, the identities of the subjects were obtained and the fraudulent profits from click fraud were traced to individuals in Estonia and Russia. It is believed that perhaps millions of computers worldwide were infected with the malware.

Working with the Estonian National Criminal Police and the U.S. Attorney's Office for the Southern District of New York, the NASA OIG and the FBI indicted seven targets on charges including computer intrusions, wire fraud and money laundering. In November 2011, six subjects were arrested in Estonia and are in the process of being extradited to the United States. A seventh target in Russia remains at large. Equally important, millions of dollars in financial accounts in Estonia, the United States, Cyprus, Denmark and Austria were also frozen, and real estate and other property belonging to the subjects were seized in Estonia.

CONCLUSION

While the DNSChanger case has not yet been adjudicated, it serves as a demonstration that the IG community can tackle these types of cases. Using NASA as a victim and tools afforded to the NASA OIG under the IG act, the case was successfully brought to indictment, numerous subjects were arrested and illicit funds seized. There are many more botnets in operation, and more are being introduced every day. In fact, if NASA's experiences are representative of worldwide cybercrime trends, the agency is receiving fewer and fewer traditional "hacker" attacks and more malware and botnet attacks, indicating that these types of investigations may be the future for IG cybercrime investigators. As noted above, the bot masters are only limited by their imagination—and to combat them, IG investigators must use all of the tools at their disposal to fight this new type of cybercrime.

Sean Zadig

Sean M. Zadig has been employed as a special agent with NASA's Office of Inspector General, Computer Crimes Division for more than six years. He has a Bachelor of Science in computer science from the University of California, a masters in criminal justice from Boston University and is a third-year Ph.D candidate in information systems at Nova Southeastern University. While at NASA, Zadig has focused on international cybercrime and malware investigations and has obtained convictions in Nigeria, China, Australia and the United States. Before joining NASA, he held positions in systems administration and software development.

Statistical Sampling: Choosing the Right Sample Size

By Dr. Kandasamy Selvavel and James Hartman Jr.

In this paper, we avoid technical terms, notations, and formulas so that persons with little or no statistical background will be able to fully appreciate the content and application of sampling in the auditing environment. We structured this paper into sections that discuss why sample, sample size for attribute projection, sample size for variable projection and sample size for internal control test.

WHY SAMPLE?

To audit all items in the target universe is generally too time consuming and prohibitively too costly. Statistical sampling when appropriately applied and implemented is an efficient tool to leverage available audit resources, thereby yielding valuable and defensible information. A non-statistical sampling approach does not allow what is found in the sample to be projected to the population, and therefore, may be considered not as efficient and effective as statistical sampling that allows sample results to be projected to the population.

The emphasis to audit in high-risk areas, with fewer resources and shorter audit cycles, further supports the need to employ statistical sampling. Consequently, auditing in this demanding environment requires improved audit planning and better audit tools to efficiently leverage resources and optimize the audit process.

At the organizational level, there is an increased emphasis on managing audits to be more timely, relevant and have a higher return on audit investment of resources. Auditing in this demanding, somewhat dynamic environment requires improved audit planning to efficiently leverage all audit resources. Statistical sampling methodology should be an integral part of the audit process, beginning in the planning phase up to supporting more comprehensive findings and recommendations.

"Statistical sampling methodology should be an integral part of the audit process..."

Statistical sampling facilitates and helps clarify the overall design, scope and what is to be measured in the audit. Statistical sampling at the beginning phase is collecting information from auditors and calculating sufficient sample size to achieve project goals, namely reportable error rate and associated dollar value with good precision.

A statistician involved early in the development of the audit benefits the process by helping ensure focus on defensible methodology of the audit and defining what will be measured in the audit. One of the most important questions asked by the auditors when they approach statisticians for consultation is the sample size. It seems like this is a simple question, but statisticians need certain information before they can provide a sample size. This includes but is not limited to the sample design, confidence level, desired precision, expected error rate and the

population size in deciding the sample size. Additional information such as distribution and size of errors improves sample efficiency.

In audit projects one of the primary objectives is to obtain useful results with minimal effort and cost. To meet this objective, statisticians analyze the population, choose an appropriate sample design and discuss the general requirements with the auditors. The statistician's aim is to determine, through calculation and experience, the minimal sample size required to sufficiently represent the population and achieve the desired precision. Unfortunately, larger samples generally produce smaller sampling error but require larger audit resources. The statistician manages this delicate balance and helps the auditor obtain useful results at minimal cost.

FIGURE 1: SAMPLE SIZE FOR SMALL POPULATION

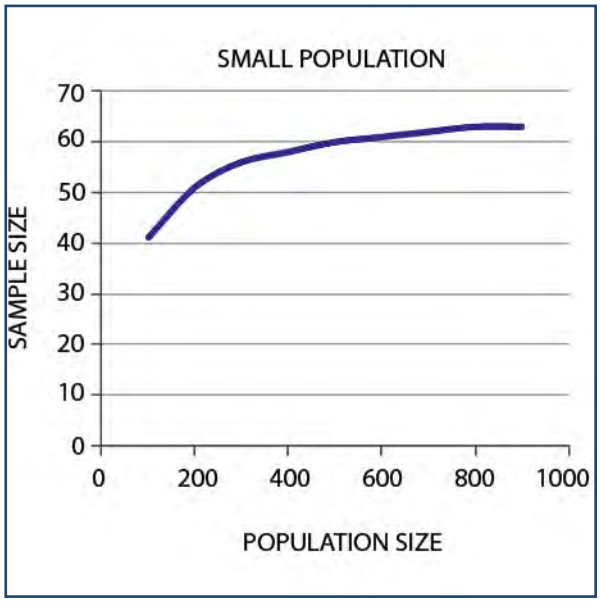
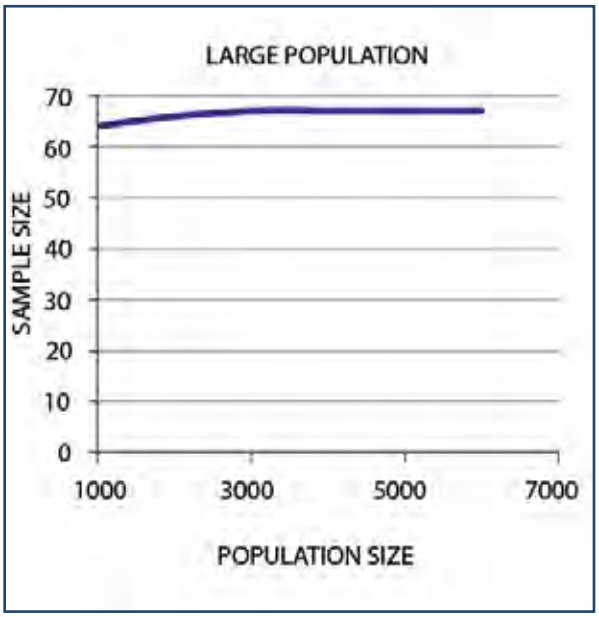


FIGURE 2: SAMPLE SIZE FOR LARGE POPULATION



SAMPLE SIZE FOR ATTRIBUTE PROJECTION

For statisticians to calculate sample size for attribute projections, they need to know what level of confidence is required in the projection (confidence level), how tight the confidence bounds need to be (precision), the population size and information on expected errors in the population (error rate). In general, a 90 percent confidence level is reasonable for the attribute projections. From past history or from a pilot study, one might be able to reasonably "guesstimate" the population error rate. When little or no information is available, a worst-case scenario (50-percent error rate) can be used to calculate the sample size. A 50-percent error-rate assumption gives the largest sample size for attribute projection.

When the population size increases, the sample size also increases, but the increase is not linear. It is important to note that the increase in sample size is minimal when the population size is very large. This is why the statistical sampling is very efficient for large populations.

SAMPLE SIZE FOR VARIABLE PROJECTION

For statisticians to calculate efficient and adequate sample size for variable projections, they need to know the confidence level, the precision, the population size and the expected standard deviation of the errors. In general, a 95 percent confidence level is used for the variable projections. To achieve a specified relative precision, expected standard

"When the population size increases, the sample size also increases, but the increase is not linear."

deviation of the errors or coefficient of variation, which is the standard deviation divided by mean, can be used in the calculation of sample size. A pilot sample or information from previous studies can be used to estimate the standard deviation of the errors. If nothing else is available, a hypothesized distribution of the population data can be used to estimate the sample size.

There are several statistical packages available for sample size calculation, but most of them do not disclose the methodologies used in their calculations. For simple sample designs, the mathematical formulae are given for sample-size calculation in many statistics textbooks. For example, see Cochran (1977),[1] Kish (2004),[2] and Lohr (2010).[3] In practice, we don't know all the values to input into the formula, and informed assumptions must be made by the statistician in conjunction with the auditor. Unfortunately, only the assumed values are known after the completion of the project. This is why calculating sample size is not an easy task for statisticians and sample sizes differ based on assumptions about the data-set and distributions. Sufficiency of the sample to adequately represent the population is mandatory for defensible statistical projection.

SAMPLE SIZE FOR INTERNAL CONTROL TEST

Minimum sample sizes for internal control tests are given in the Government Accountability Office Financial Audit Manual for large populations

FIGURE 3: THE POPULATION AND THE SAMPLE SIZE FOR INTERNAL CONTROL TEST

Population Size (N)	Sample Size (n)	Population Size (N)	Sample Size (n)
up to19	all	60-67	29
20	14	68-70	30
21-22	15	71-72	31
23	16	73-102	32
24-32	17	103-150	33
33-34	18	151-154	34
35-36	19	155-159	35
37-38	20	160-195	36
39-40	21	196-200	37
41-42	22	201-206	38
43	23	207-228	39
44-45	24	229-234	40
46-47	25	235-290	41
48-49	26	291-336	42
50-51	27	337-500	43
52-59	28	501-2000	44

1) Cochran, W.G. (1977). Statistical Techniques. 3rd., New York, N.Y: Wiley.
2) Kish, L. (2004). Statistical Design for Research. Hoboken, N.J.: Wiley.
3) Lohr, S. L. (2010). Sampling: Design and Analysis. Pacific Grove; CA: Duxbury.

"Clarity of the audit objective(s) facilitates the design process and enhances the statistician's ability to develop a more efficient design, and ultimately, to obtain more useful audit results."

greater than 5,000. The control test sample size table provided in FAM is based on a 90-percent confidence level and 5-percent tolerable error. The auditors should rely on statisticians to calculate the sample size for small population.

For internal control tests, we present the sample size table for small populations of 2,000 or less. Our sample size calculations are based on the theory given in Wendell and Schmee's paper.[4] They use the hypothesis testing approach in their methodology. Because of the discrete nature of the hypergeometric distribution, it is not possible to calculate the exact sample size for very small populations less than 100 that yields 5 percent upper bound. Therefore, for some very small populations, the corresponding upper bound varies from 3 to 6 percent. Figure 1 presents sample sizes calculated based on 90-percent confidence level and 5-percent tolerable error.

The Decision Rule for the control test: If zero exceptions are found in the sample, this indicates we are at least 90 percent confident there are no more than 5 percent of the items with exceptions in the universe. Therefore, we accept the null hypothesis that there are no more than 5 percent errors in the universe and conclude controls are working.

CONCLUSION

After the audit topic is defined and scope of the audit is developed, statisticians can assist in defining the population and establishing the target precision and the allowable level of audit risk. The audit risk is the complement of the level of confidence and is determined either by published guidance or in consultation with the statistician and audit management. If management is willing and in a position to offer additional resources and more time for the audit process, then the statistician can design a sample with lower risk, a higher confidence level and better precision.

Clarity of the audit objective(s) facilitates the design process and enhances the statistician's ability to develop a more efficient design, and ultimately, to obtain more useful audit results. To optimize resources for any sampling design, the appropriate goals and objectives of the audit must be clearly defined. Usually, multiple objectives can be managed and addressed with minimum impact on audit resources within the same sample design.

The auditors are often interested in reporting a point estimate. The point estimate should be given only with the corresponding standard errors or the confidence interval. The standard error gives some measure about the quality of the calculated estimates. A point estimate with very wide confidence

4) Wendell, J. P. and Schmee, J. (1996). Exact Inference for Proportions From a Stratified Finite Population. Journal of the American Statistical Association, 91, 825-830.

interval may be less useful for decision makers than the point estimate with narrow confidence interval. That is, a smaller precision is preferable.

The challenge is to provide defensible decisions using the statistical projections. A useful approach is to compare the decision that would be made at each of the confidence bounds. That is, would the decision or conclusion differ if the true errors were at the lower versus the upper confidence bound? If so, a degree of comfort is gained in reporting or using the estimate. If the decision or conclusion at each confidence bound is different, then additional information may be needed to make a reasonable conclusion. ☙

Dr. Kandasamy Selvavel

Dr. Kandasamy Selvavel has more than ten years of statistical consulting and oversight experience with the Department of Defense Office of Inspector General. Selvavel has published more than 20 research papers in various professional journals. Prior to joining OIG, Selvavel worked for more than three years as a mathematical statistician at the Census Bureau. He also taught several college level mathematics and statistics courses at universities for more than 10 years prior to joining government service. Selvavel holds Master of Arts and Doctor of Philosophy degrees in mathematics with majors in statistics from Bowling Green State University, Ohio.

James Hartman Jr.

James D. Hartman Jr. has been the technical director for the Quantitative Methods and Analysis Directorate of the Department of Defense Office of Inspector General for three of his 12 years with the agency, providing statistical and quantitative support for numerous types of projects.

In 2004, Hartman was detailed to the Coalition Provisional Authority IG and deployed to Iraq to provide statistical support for audits, inspections and investigations. He is a certified ISO-9000 assessor/lead assessor. His undergraduate degree is in experimental psychology from Wofford College, Spartanburg, S.C. Hartman has a Master of Business Administration from the University of South Carolina, Columbia, and he did doctoral work at Clemson University, S.C., in industrial management.

Conceptual Framework for Grant Oversight Using Data Analytics

By Dr. Brett Baker

In fiscal year 2011, 26 federal agencies provided approximately $600 billion in federal financial assistance to more than 80,000 recipients. Approximately 1,600 of the grant programs funded in 2011 supported national infrastructure, scientific research and cultural enrichment activities that are designed to promote the public good.[1] A federal grant is an award of financial assistance from a federal agency to carry out a public purpose of support or stimulation authorized by a U.S. law. Recipients must expend the federal grant funds in compliance with federal regulations and in the execution of the programs and activities detailed in grant documents. Oversight of those funds is challenging as there is limited information available to ensure costs are reasonable, allocable and allowable.

The Conceptual Framework for Grant Oversight Using Data Analytics describes an oversight approach that emphasizes the use of automated techniques in the planning and execution processes for grant oversight. Data obtained from multiple databases can be compared and analyzed to identify anomalies in recipient federal award cost data and award-expenditure patterns. Such techniques allow oversight officials and Offices of Inspectors General to expand coverage of the grant dollars, increase the accuracy of analysis, improve the efficiency of planning, and ultimately, reduce the time and cost of conducting a review. In addition, automated techniques can provide transparency of recipient spending that is difficult and challenging to see using traditional oversight techniques

"Data obtained from multiple databases can be compared and analyzed to identify anomalies in recipient federal award cost data and award-expenditure."

The framework provides auditors and investigators a risk-based, data analytics-driven approach to identify institutions that may not be using federal funds in accordance with the Office of Management and Budget cost principles, administrative rules or within the terms and conditions of their federal award agreements. The framework also demonstrates how oversight organizations can integrate agency, recipient and open source information to provide a more comprehensive view of risk rather than using traditional risk identification techniques, such as statistical sampling.

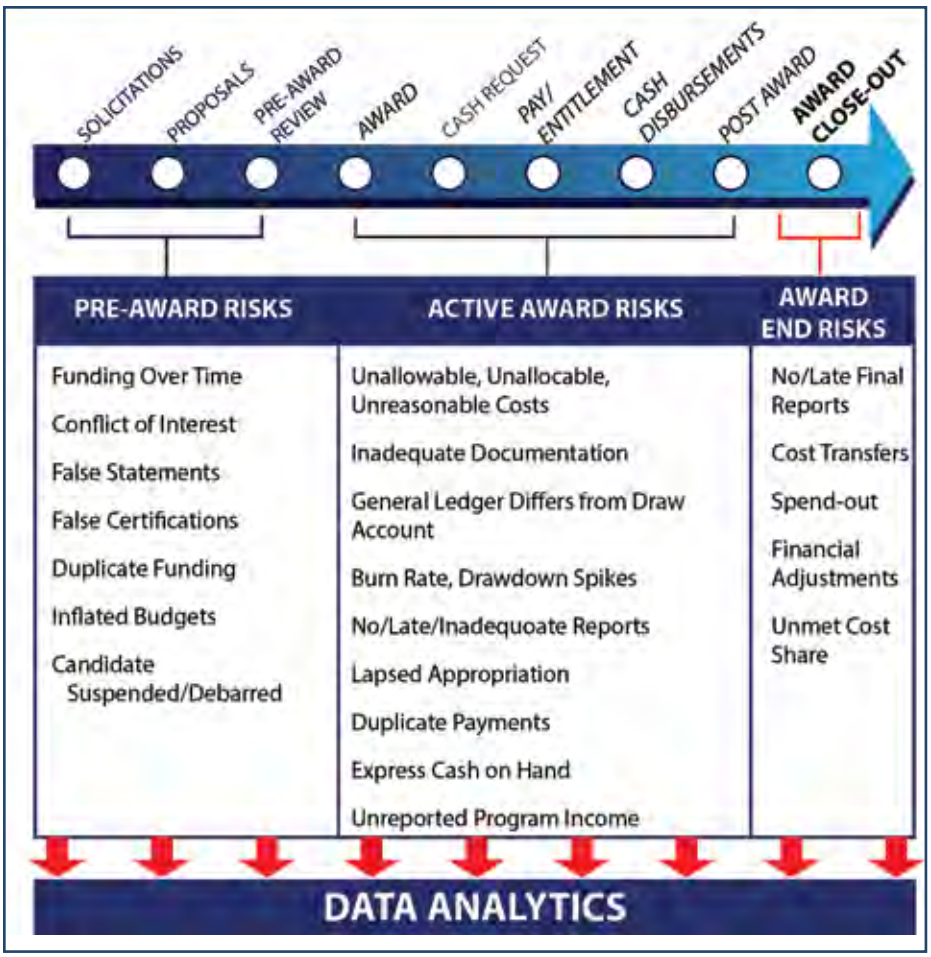
Lastly, the framework offers a methodology to enhance the audit and investigative capabilities for all offices, regardless of staff size. Automated techniques to review data sets can increase audit oversight from a sample of transactions to 100 percent coverage of all transactions and can provide continuous auditing capabilities. Audit planning efforts can identify expenditure anomalies by comparing databases, reviewing more data/transactions and evaluating risk areas. Accordingly, audit and investigative work can be targeted to areas of risk identified through targeted review planning; thus, the time and resources required to determine whether the grantee's use of the grant funds met federal and agency requirements can be reduced.

1) www.grants.gov.

GRANT RISKS THROUGHOUT THE AWARD LIFE CYCLE

Life cycle oversight can be accomplished through automated techniques to monitor agency-award systems and external data. The three main phases in the life cycle of grants are pre-award, active award and award end/closeout. Each federal grant-awarding agency compiles financial and award information that can be reviewed with data analytics to identify anomalous activities and changes in activity over time.

FIGURE 1: CONCEPTUAL FRAMEWORK FOR GRANT OVERSIGHT



In the pre-award phase, the grant process may begin with a solicitation for proposals to address an agency program or interest area. During this phase, agencies must guard against bias that might result from a conflict of interest, such as panel members who have relationships with key proposal personnel or the requesting recipients. Common pre-award risks include:

- Funding over time involves project grants that are awarded through a competitive process where success rates traditionally range from 20 percent to 30 percent.[2] Significantly higher success rates by an institution or principal investigator would be a potential indicator of risk of weak controls over the award process. This risk can be identified through analysis of award decisions in agency award information systems.
- Conflicts of interest involve a recipient or someone with an undisclosed relationship to a prospective recipient or project, or someone who may have an undisclosed financial interest, personal interest or professional interest in that project. Conflicts of interest include financial investments that could increase in value should a project be financed, or a relative could be part of the award-decision process. This risk can be discovered through an analysis of agency award systems.
- False claims, certifications and statements are representations made verbally and/or in writing by awardees to falsify or conceal a material fact. Penalties under the Federal False Claims Act[3] for false representations can be three times the loss to the federal government (treble damages). Data analytics can help uncover issues that result from false statements by displaying transactions that do not comport to the statement.

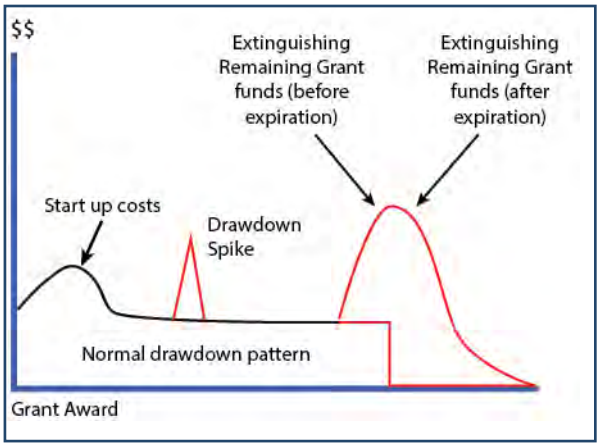
2) www.research.gov.
3) Federal False Claims Act (31 USC 3729-3733) imposes liability on any person or organization who submits a claim to the federal government that he or she knows (or should know) is false.

- Duplicate funding can occur when candidates send proposals to multiple agencies to increase funding chances. There is a risk that multiple agencies will fund the same work. Data analytics of award abstract information from online resources such as www.grants.gov can identify potential duplicate funding.
- Inflated budgets can occur if a proposal budget requests a higher dollar amount than is needed. The extra funds may be used for non-grant purposes. Comparisons of similar awards within agency award systems can identify potential award-budget anomalies.
- Candidates suspended or debarred can be discovered through the System for Award Management website at www.sam.gov, which links to the Excluded Parties List System website that provides a list of individuals and entities excluded from doing business with the federal government. A suspension or a debarment is a temporary prohibition against an institution to participate in federal award programs, including receipt of funding and seeking new awards. Data analysis of suspension and debarment information against agency award systems can identify institutions that should not be participating in award programs.
- High-risk grantees include prospective or existing grantees who may be experiencing challenges that result in financial instability; may have inadequate system of internal controls or management controls; or have not conformed to the terms or conditions of previous awards. As a result, a grant could be awarded without the benefit of any special conditions or requirements to mitigate the high-risk conditions if the awarding agency fails to consider and address adequately high-risk indicators during the pre-award process. The Federal Audit Clearinghouse is a repository for OMB Circular A-133 Single Audit Act annual audits and is a source of data that can show these weaknesses. Comparison against agency award-information systems can identify higher risk institutions.

During the active award phase, recipients expend grant funds throughout the period of performance, which can range from one to five years. Recipients request reimbursement payments from the awarding agency generally as an aggregate dollar amount. Unlike contract payments, federal agencies do not receive an invoice or other billing detail to support the expenditures. While recipients provide quarterly, annual and final reporting, those reports do not detail how the grant funds were expended. The following can apply during the active award phase:

- Audits conducted under OMB Circular A-133 Single Audit Act provide some level of oversight regarding internal controls for recipients who report expenditures of at least $500,000 per annum, but the scope of financial and compliance testing is limited. Thus, unallowable use of federal funds may not be discovered in these audits.
- Unallowable costs are those costs that are not allowed by OMB Circulars and/or by federal award terms and conditions. Unallocable costs are those that clearly do not meet the purpose or intent of the award. Unreasonable costs are often excessive charges or unnecessary costs. Unallowable, unallocable and unreasonable costs are generally reported as questioned costs as part of OIG and A-133 audits. Data analytics of awardee general ledger information can readily discover these costs.

FIGURE 2: ANAMALOUS GRANT FUNDS DRAWDOWN PATTERN



- Inadequate documentation includes inconsistent (or consistent) labor charges, use of a ghost employee or the addition of an unallowable percentage against the grant. Federal awards require awardees to maintain proper cost documentation to support award expenditures. Receipts are required for purchases of materials, equipment and supplies, and labor

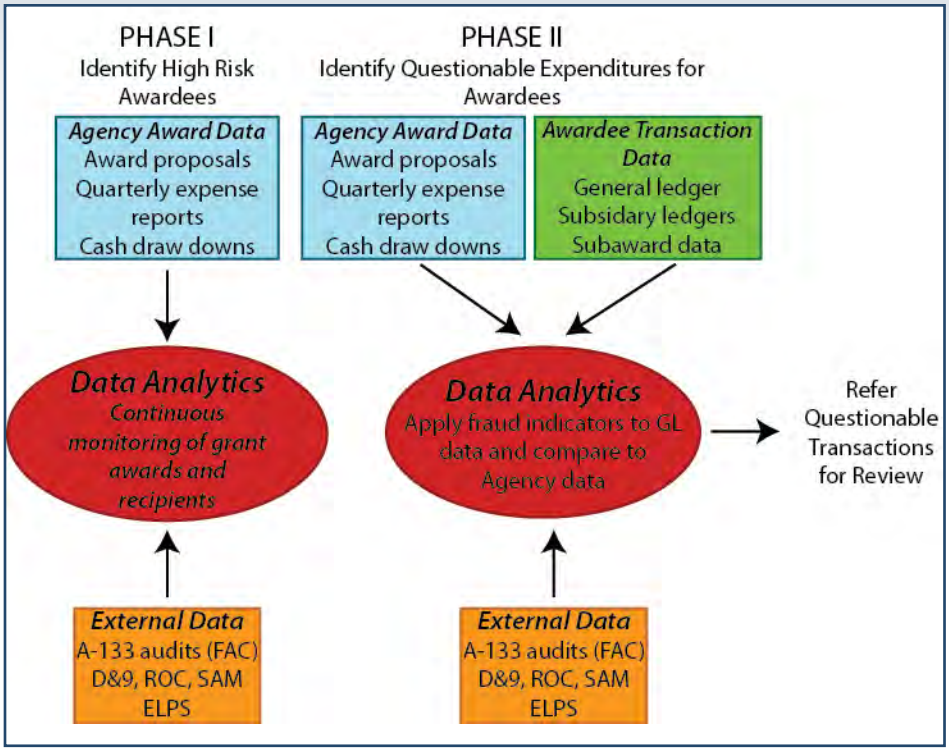
charged to the project must be properly documented.

- Awardee general ledger differs from cash-reimbursement draw requests: Comparing awardee financial information for cash reimbursement draw requests to agency payment systems can readily identify anomalies. Differences may indicate funding was used for non-grant purposes or excessive levels of cash on hand.
- Abnormal cash reimbursement, such as unusual spikes in amounts or increased frequencies of cash reimbursement requests could be drawdown patterns that may be indicative of requests to cover nonaward needs of the recipient. Spikes in cash reimbursement requests can indicate that funds may not be used fully for the purposes of the award. For example, an institution that makes a large, atypical cash reimbursement draw at the end of the month or quarter may be using the funding to meet operational cash needs rather than the award. Spend-out charges near the end of an award or after the award may warrant even greater attention. These patterns are visible in agency-payment system data, and award activity can be charted.
- Inadequate recipient reporting, such as late or no program and financial reporting to the agency are strong indicators that the project may not be progressing in accordance with the terms of the award and that funding may not be used only for the award. This information is available in agency financial and program award system data.
- Contracts, subcontracts and consultants increase risks because parties other than the primary grantee control and expend grant funds. Grants budgeted for multiple contracts and consultants, and/or with large dollar amounts flowing to other parties should be identified for review.
- Potential duplicate and improper payments can be seen in the agency financial system data as exact amounts usually requested within a short time period. Office of inspector general staff can examine the supporting payment documentation to ascertain whether these exact dollar amounts truly are duplicate payments.
- Excess cash on hand, such as cash requests that exceed the needs of an awardee are difficult to see in agency financial system data but can surface in data analysis of awardee financial information. Duplicate payments also can provide excess cash.
- Unreported program income is income from the project that is not reported on the Federal Financial Report, the annual report and/or the closeout report. This can be identified through an analysis of awardee general ledger information.
- An OMB Circular A-133 Single Audit may not be required for recipients who receive, from multiple agencies, individual federal awards that are below the current $500,000 reporting threshold, but the aggregated awards may meet the requirement for an A-133 Single Audit to be performed. An analysis of Federal Audit Clearinghouse data against agency award systems and data available in www.grants.gov can readily identify unmet Single Audit requirements and audit finding trends for the institution.

During the award end and closeout phase, no further costs are allowed to be incurred after the period of performance for a grant has ended. Thus, the recipient is responsible for reporting total expended award funds to the awarding agency, both to close the agency's award financial account and as part of the final project report that describes the results and benefits of the project financed with federal award funds. The following can occur:

- Inappropriate cost transfers are seen within awardee financial information. A-133 audit testing may provide insight into the potential risk of inappropriate cost transfers. Awardees may use funds from one award with excess funds to cover costs on other awards that have extinguished the funds. Data analysis of awardee general ledger data can uncover inappropriate movement of funding between awards from a single federal agency as well as awards between federal agencies.
- Lack of final reporting or late reporting indicates higher risk awardees because the awardees have not provided timely information on their federal program. This information can be found in agency financial and program award systems data.
- Funding drawdowns within the last month of an award and requests made after the award

FIGURE 3: DATA ANALYTICS FOR GRANT OVERSIGHT



expiration are higher risk transactions, particularly when request levels spike dramatically from their normal patterns. Funding requests can be seen in agency systems as well as in awardee financial systems data. Expenditures for equipment and materials at the end of an award or after its expiration date can often be unrelated to the purpose of a federal award and are questionable.

- Financial adjustments should be identified and reviewed, which includes unusual dollar amounts, numbers of adjustments, timing of adjustments and cost transfers to or from other accounts. Data analysis of awardee general ledger information can show anomalous financial adjustments.
- Cost sharing is an award requirement to provide a percentage of nonfederal funding to obtain the federal funds. Awardee matching fund information must be validated in the awardee financial systems data. Data analysis of awardee general ledger information can show unmet cost share by the recipient.

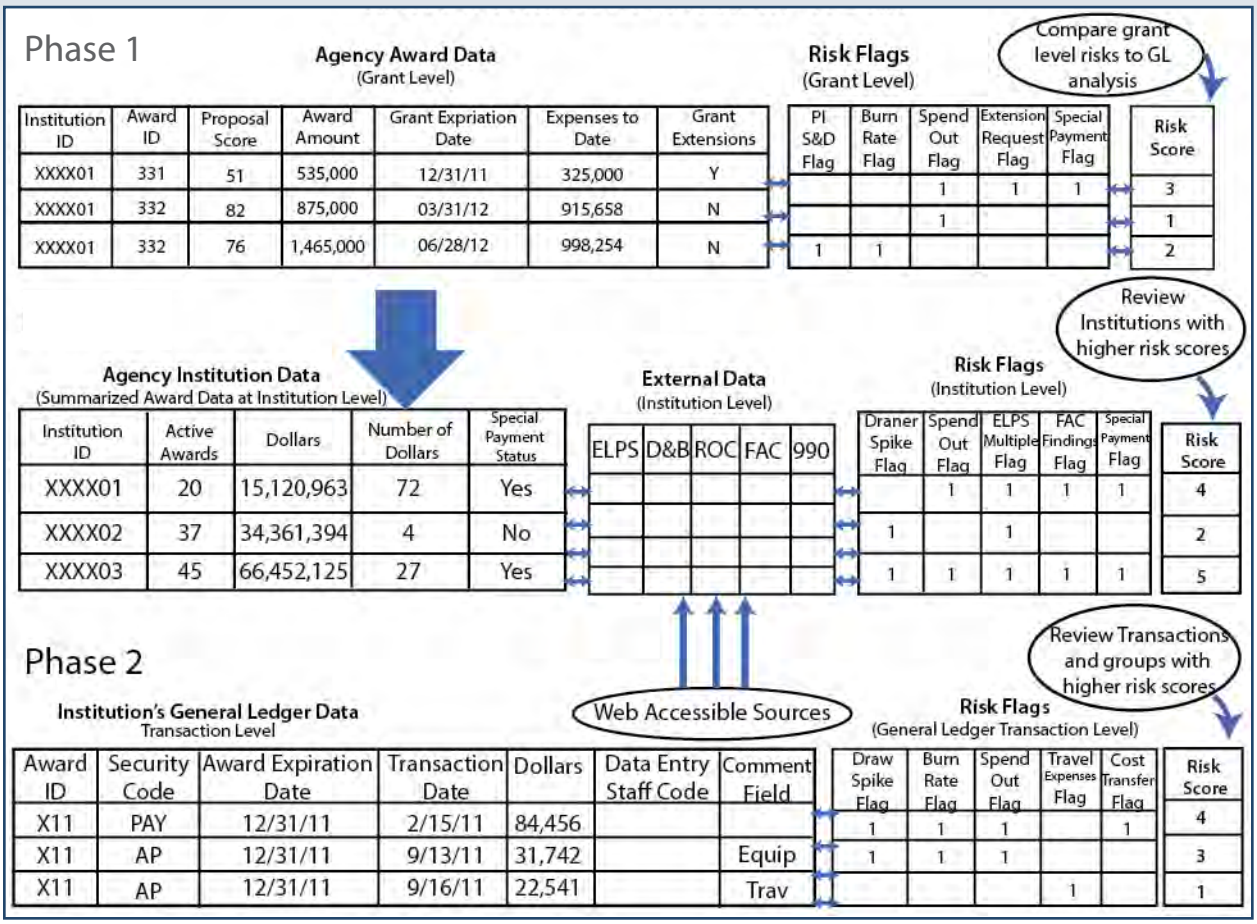
DATA ANALYTICS FOR GRANT OVERSIGHT

The framework provides an alternative approach to auditing by emphasizing the use of automated techniques in the audit planning process as well as providing a way to uncover questionable transactions during fieldwork. The framework for grant oversight provides agencies, auditors, and investigators with a data analytics-driven methodology to identify recipients that may not use federal funds properly and to perform life cycle oversight. Data from multiple databases can be compared and analyzed to identify anomalies in recipient federal award cost data and expenditure patterns. At the end of an engagement, it is important to determine the usefulness of the grant fraud indicator(s), i.e., what worked and what did not work in the data analytics process to help refine the modeling. False positives (transactions that look unallowable but are allowable) can be reduced by providing feedback to the data analytics and modeling team.

PHASE I – IDENTIFICATION OF HIGHER RISK INSTITUTIONS

Agency proposal and award data combined with externally available information can show awardee activity over time, including anomalous patterns. Agencies maintain grant proposal and award financial information at the grant-level and institution-level as part of their award and post-award monitoring efforts. This includes information, such as proposal narratives, panel scoring, quarterly reports, drawdowns and closeout reconciliation. This information can be extracted into an OIG database and combined with other open-source information, which is available on the Internet, to produce an institution risk profile that can be compared

FIGURE 4: RISK IDENTIFICATION FRAMEWORK



against other institutions to surface outliers. Actual expenditures by awardees are not readily visible to agency officials. Unlike contract payments, requests for financial assistance award funds are not normally accompanied by supporting documentation, such as invoices and receipts—this level of detail is available during the framework's Phase II testing of awardee general ledger information. Information that is visible to awarding agencies often only includes lump sum cash drawdown requests without specific information about the underlying grants. The primary control agencies can apply to summary funding requests is to compare the amount of the funding request against remaining balance of open awards before making the disbursement. If there are sufficient funds, the agency can make the disbursement. If funds are not sufficient, the awarding agency contacts the institution. Summarized funding requests can still provide useful insight for identifying potentially risky payments, such as expenditures unrelated to a federal award. Auditors and investigators can examine payment history over time to look for drawdown spikes, which can be an indicator of institutions using federal funds to cover the cost of institution operations, and not authorized grant activities. This is particularly true if funding requests occur around common financial reporting periods, such as end of the month, quarter, or year.

Federal Financial Reports capture grant expenditures at a summary level for the previous quarter by grant award. The automated reports provide high-level information on grant spending and reconciliation information that agencies use to make adjustments to award funding requests made during the quarter. While the FFR data is reported in 90-day increments, it still provides spending-pattern information. For example, a last-quarter FFR with higher than normal funding expenditures can be an indication of an awardee spending out the remainder of an award's grant funds for purposes other than the terms and conditions of the grant. It

may also be an indicator that funds were spent after the award expiration date as FFRs are not normally submitted in quarters after the award has expired. Those expenditures may have been collapsed into the last FFR for the grant. FFRs that are in database formats are another valuable tool to identify potential misuse of federal funds. Award management and financial information are additional ways to gain insight on awardee risks. Special payment and late reporting information can signal higher risk activities by an awardee. Careful examination of the information provides auditors and investigators with an additional capability to identify institutions that may not be using federal funds properly.

Externally available data, such as institution-level information is captured by a number of organizations within and outside the federal government. As noted previously, reports completed under the requirements of the A-133 Single Audit Act are maintained in the Federal Audit Clearinghouse and can be compared with agency financial and program award information to provide additional risk information. Dun and Bradstreet has financial information on most entities within the U.S. and also maintains financial risk scores, which can provide valuable insight on an institution's financial stability. The Excluded Parties List System maintains information on institutions and individuals who have been suspended or debarred from performing on federal contracts or grants. The ELPS includes current and historical information. Current matches against the ELPS would be a signal that the institution should not be doing business with the government. A historical match would provide a valuable indicator of potential risk that funds may not be used properly by the institution. The System for Award Management provides organizational and operating information on contractors and grantee institutions that wish to do business with the federal government. Information from the various sources can be refreshed periodically. Key to combining agency data with externally available open-source information is a way to link the data from the various files. This normally is an institution identifier such as an entity identification number, D & B's Data Universal Numbering System and/or a commercial and government entity code from the SAM. Data from these external sources is generally available through Web-accessible portals and download functions.

Establishing a data repository to compile federal award and federal awardee data from multiple sources (both internal and external to the award-granting agency) provides a capability to assign risk to its awards and award recipients. This central repository, coupled with the use of data mining techniques, will allow the examination of all available records related to a specific federal award or federal award recipient rather than just a sample. It will also facilitate comparisons of data from multiple systems to create data relationships, perform comparisons and other analytics, summarize large volumes of data, and identify anomalies and trends over time.

Agency data (grant level) is the initial step in building a data repository by constructing a database of agency award data at the individual award level. This data includes pre-award data from institution proposals that show panel scoring results (individual scores, and summary), detailed cost categories from award budgets and funding changes throughout the panel review process. The repository would also include agency award information throughout the active award phase of the grant, such as, cash reimbursement-request history and cash draw patterns, burn rate (how quickly an awardee spends its grant funds), special payment flags, etc. Individual grant risk indicators can be developed for these kinds of risks and applied to the database to provide a grant-based risk score that is helpful for on-site grant audit and investigative teams to focus their attention during their work.

Individual grant awards for an institution can be summarized at the institution level to allow for comparisons against external data sources, such as, ELPS, SAM, FAC, and D&B databases. This comparison allows for the development of institution-level risk flags and a composite score that auditor and investigative teams can use to identify higher-risk institutions.

The detailed testing of institution detailed transaction level data from general ledgers provides the most compelling evidence for identifying potentially questionable costs for audits and investigations. Risk indicators of high-risk conditions can be coded into the data analytics tools and databases to show inconsistencies in cost transfers, inappropriate equipment purchases, ghost employees, etc.

The oversight database can be analyzed with any number of data analytical tools. Common audit applications such as ACL, IDEA and Microsoft Access can combine data files and perform data field analysis to surface anomalous activity. More sophisticated applications such as SAS Enterprise Miner and IBM Modeler have data mining features that can surface underlying anomalies and patterns within the financial and program information that warrant further attention. The tools can examine data fields for outliers and anomalies, both within a database and activity over time. Additionally, the tools can produce risk-based profiles on several levels, e.g., grant-type, institution-type, drawdown frequency. These tools can develop institution profiles that show normal financial and program behavior, e.g., drawdown frequency and amount. The data analysis applications can also provide additional insight into risky activity such as unusual bank account changes and special payment status. The resultant continuous auditing database essentially provides a list of all institutions (rows) and fields (columns) with the scoring results of the various indicators, some of which would be weighted higher or lower, based on risk. The sum of the indicator risk scores creates a composite risk index for the institution that can be used to compare institutions as depicted in the Risk Identification Framework on page 55. While a single risk indicator can provide important insight, a composite risk indicator developed by combining several single risk indicators provides even greater visibility of anomalous activities and potential risks.

PHASE II — DATA ANALYTICS DRIVEN REVIEW APPROACH

This standardized review approach applies to steps that occur after an awardee has been selected, and it will help to identify highest-risk areas and transactions related to an awardee, which should be reviewed and audited. The steps in this process are:

First, it is necessary to obtain automated awardee financial and program data and compare that to agency data. By obtaining large amounts of data (e.g., the general ledgers for all awards from a particular Institution) and comparing an awardee's data to agency data, it is possible to identify quickly and efficiently any discrepancies that exist. Further, by using automated techniques, this process includes a 100 percent automated review of the transaction-level data for awards from that agency. The discrepancies indicate the areas in which to focus attention. For example, if there are large differences between amounts of expenditures recorded in the general ledger for a particular project grant and the amount reported to the agency for that grant, that grant would at least warrant further scrutiny.

Although comparing general ledgers to spending reports submitted to the agency are routine audit steps, automating the process would enable the selection of potentially higher-risk grants at the outset, whereas in traditional audit processes, the comparison of grantee and agency data occurs after particular grants are selected for audits based on other criteria, such as large dollar amounts in known high-risk budget categories.

Second, it is necessary to perform analytics on awardee data to look for anomalies, such as the unusual spending patterns presented in the Grant Risks Throughout the Award Cycle section and illustrated in the Conceptual Framework for Grant Oversight chart. Obtaining grantee data can identify transactions that may circumvent the requirement to return unused funds to the agency, such as cost transfers from expiring awards to awards that are open or expenditures of unused funds at the end of the grant for budget categories that did not support the work of the grant.

Automated analytical tests of general ledger information can uncover questionable expenditures that review teams can perform in-depth testing on to determine what is allowable, allocable and reasonable. Large operational equipment purchases near the end of a grant's expiration date are a strong indicator that funds are not being used for the purposes of the grant. Excessive and inappropriate travel expenditures are also visible in institution general ledger information, such as, frequent foreign travel with first-class seating and high-end lodging accommodations. Analytics can also discover expenditures charged to one federal agency's grants that are actually for other federal awards received by that same institution. Testing can be conducted to identify excessive cash draws early in the award that institutions use for purposes not related to the grant. This is important because federal grant funds are not intended to provide institutions with an interest-free line of credit to fund other activities.

Indeed, testing an institution's general ledger data against agency information can provide im-

portant award expenditure information that would not surface using traditional grant auditing techniques. This occurs because using automated tools and techniques allows a 100-percent review of the data and provides a powerful way to surface potential misuse of federal funds. A 100-percent review is in contrast to the traditional financial-assistance audit that uses statistical-sampling approaches, which would result in examining fewer transactions and lower-questioned costs. Testing against external data also helps corroborate and validate risk areas identified through earlier comparisons with the A-133 FAC, D&B, SAM and EPLS databases. By comparing agency financial and program data against external data sources and the institution's general ledger data, offices of inspectors general can provide greater oversight of federal funds at an institution.

CONCLUSION

In summary, using data analytics throughout the grant life cycle can provide oversight organizations with greater visibility and insight into how institutions are using federal funds resulting in greater accountability and transparency. Data analysis of agency award information, combined with available external and awardee data can help identify higher risk institutions for planning purposes as well as surface anomalous and questionable grant expenditures during audit work. While offices of inspectors general can enhance their oversight using the framework for grant oversight, other oversight organizations within federal agencies can also benefit from the approach. Collectively, these organizations can provide greater assurance to the public that government funds are being used appropriately.

ACKNOWLEDGMENTS

Thanks to Laura Koren, Jayne Hornstein, Jennifer Miller and Emily Woodruff, National Science Foundation OIG, for their assistance in preparing this article and to Della Whorton, Recovery Accountability and Transparency Board, for her thoughtful review and comments. Special thanks to Allison Lerner, NSF inspector general, for her leadership and continued support in promoting data analytics and automated oversight throughout the federal government.

Dr. Brett Baker

Dr. Brett M. Baker is currently the assistant inspector general for audit, responsible for directing a program of oversight audits and evaluations of the National Science Foundation's annual financial statement and the performance and financial aspects of NSF programs, activities and awards. Baker previously was the AIGA at the Department of Commerce Office of Inspector General, where he provided direction and oversight to auditors and inspections staff performing financial statement, financial-related, and performance audits and evaluations. Prior to that, Baker was the director for internal review with the Defense Finance and Accounting Service where he was responsible for providing audit and investigative oversight for more than $600 billion in Defense financial management operations. Before his work with Defense, he was the director for systems internal audit at the Department of Education OIG, where he was responsible for directing technically complex system audits and data analytics engagements.

Baker has been honored for his contributions to the OIG community, receiving Awards for Excellence from the President's Committee on Integrity and Efficiency in 1998 and 2003, and from the Council of the Inspectors General on Integrity and Efficiency in 2011. He received the National Science Foundation Director's Award for Collaborative Integration in 2011. Baker also serves as the chair of the Federal Audit Executive Council and is a member of the Department of Defense Office of Inspector General Audit Advisory Committee. He also serves on the Information Technology Advisory Panel for the Government Accountability and Transparency Board. Baker has also authored articles on data analytics and data mining for the Journal for Public Inquiry (2009) and the Global Digital Business Review (2006).

Baker earned a Ph.D in information technology management at the University of Maryland University College in 2007 and a master's degree in information resource management at Central Michigan University in 1998. He holds a Bachelor of Arts in accounting from the University of Northern Iowa and a Bachelor of Science in sociology from Iowa State University. Baker is a certified public accountant and certified information systems auditor.

DoD Efforts to Achieve Audit Readiness and Obtain an Unqualified Opinion

By James Davis Jr

The Department of Defense is currently unable to obtain any opinion, let alone an unqualified opinion,[1] on its financial statements because it is not "audit ready." Why is achieving auditability important? "The need to produce a financial statement and achieve a clean audit opinion" leads to better financial management.[2] Financial statements are a documented form of transparency and accountability. Certainly, "transparency and accessibility of public information in the promotion and maintenance of public sector accountability" is of great concern to public administration and management scholars.[3]

However, these scholars as well as the American public could learn from the use of financial reports. Public officials are to be proper stewards of the citizens' trust and resources. In these tough economic times, senior leaders need to make difficult budgetary decisions based upon reliable, timely information. Therefore, outside observers, like the American taxpayer, should be knowledgeable about how civil servants at DoD spend their tax dollars. We all have a vested interest in achieving a successful outcome. Yet, studies suggest that decision-makers do not use federal financial statements to make decisions, and that DoD's problem with CFO Act compliance can be traced back to accounting practices and philosophies under Secretary McNamara's administration.[4]

Nevertheless, DoD has continually been given a disclaimer on its financial statements, due to at least 13 uncorrected material weaknesses in the areas of financial management and feeder systems, Fund Balance with Treasury, Accounts Receivable, Inventory, and General Property, Plant and Equipment. Since DoD as an agency is material to the overall federal government, the federal government cannot obtain an opinion on its consolidated financial statements. In addition, once DoD is auditable and obtains an unqualified opinion, the DoD would be "better positioned to have accurate and timely information on a daily basis to ensure that every dollar supports the warfighters, improves military readiness and is readily available to key decision makers."[5] Therefore, achieving audit readiness is of the utmost importance.

EVIDENCE (CAUSES)

DoD, as a whole, has never achieved an unqualified opinion on its financial statements, because it is not "audit ready." GAO reported that "DoD financial management has been on GAO's high-risk list since 1995, and despite several reform initiatives, it remains on the list today."[6]

DoD is not ready for a full financial statement audit because of the following:

- Changes in leadership and priorities.
- Lack of an effective plan to address internal control weaknesses.
- Lack of an adequately trained financial management workforce.
- Ineffective "accountability and oversight."

1) According to Wikipedia, an unqualified opinion is an opinion when "the auditor concludes that the financial statements give a true and fair view in accordance with the financial reporting framework used for the preparation and presentation of the financial statements" (Retrieved from en.wikipedia.org/wiki/, p. 1, searched January through March 2012).
2) Brook, D., (2010). Audited Financial Statements in the Federal Government: Intentions, Outcomes and On-going Challenges for Management and Policy-making. *Journal of Public Budgeting, Accounting & Financial Management, 22(1),* p.61.
3) Kioko, S., Marlowe J., Matkin, D., Moody, M., Smith D., and Zhao, Z. (2011). Why Public Financial Management Matters. *Journal of Public Administration Research and Theory, 21, p.* i116.
4) Hanks, C., (2009). Financial Accountability at the DoD: Reviewing the Bidding, pp. 184-6.
5) Department of Defense Agency Financial Report for FY 2010 , p. 32, and Blair, D., (2011). Statement of Daniel R. Blair, Deputy Inspector General for Auditing, DoDIG, before the Subcommittee on Government Organization, Efficiency and Financial Management, Committee on Oversight and Government Reform, on "Financial Management and Internal Control Challenges at the Department of Defense," pp. 3 & 19.
6) GAO-11-864T (2011). *DoD Financial Management: Numerous Challenges Must Be Addressed to Achieve Auditability*, p. 1.

- Lack of a "well-defined enterprise architecture."
- Delays in enterprise resource planning system implementation.[7]

The Brook Study found that many agencies "achieved clean audit opinions by applying extraordinary effort to key problem areas." Extraordinary effort was defined as "the employment of large numbers of personnel to accomplish tasks that the current systems and procedures cannot manage." Examples cited include "assigning task forces of extra personnel, hiring contractors, etc." However, "heroic effort" could be "expensive and difficult to sustain." Therefore, gaining and maintaining a clean opinion may not be an option.[8]

"... obligations made during execution to provide for national security in the future, not the historical costs tracked by private sector-style financial accounting."

GAO noted that "improvements to DoD financial management would require the involvement of DoD operations performing other business functions that interact with financial management, which includes higher-risk areas in contract management, supply chain management, support infrastructure management, and weapons system acquisition."[9] DoD officials acknowledged that "sustained and active involvement by the DoD's chief management officer, the deputy chief management officer, the military departments' chief management officers, the DoD comptroller and other senior leaders is critical." GAO indicated that "within every administration, there are changes at the senior leadership." Therefore, involvement across DoD and at all levels is necessary for achieving a positive outcome.[10]

Still, Dr. Christopher Hanks, a defense analyst, repeats the argument first made by former DoD Comptroller Robert Anthony that the DoD's decision-making is more driven by "world events, politics and the budget."[11] Hanks makes an additional argument that DoD would focus on addressing "obligations made during execution to provide for national security in the future, not the historical costs tracked by private sector-style financial accounting."[12] Although Hanks suggests that DoD should move toward a managerial accounting approach to aid internal users to control costs, he also points out that the Association of Government Accountants' 2008 CFO Survey revealed that federal executives and managers do not use financial statements to make decisions.[13] Therefore, senior leaders at DoD need to become more involved in Chief Financial Officers Act compliance.

According to the Brook Study, agencies with demonstrated senior leadership commitment have achieved more clean audit opinions. This was determined to be "the single, most important management factor in achieving clean audit opinions." The study concluded that "agency leaders who decide that producing a reliable audited financial statement is an organizational priority can direct resources and energy into that area and hold managers accountable for achieving that goal."[14]

Secretary of Defense Leon Panetta, has quickly become involved in accelerating the readiness effort. In an October 2011 memorandum, he directs the DoD comptroller to "provide a plan to achieve audit readiness for the Statements of Budgetary Resources by the end of 2014, increase emphasis on accountability for assets, execute a full review of DoD's financial controls over the next two years and establish interim goals to assess progress, ensure mandatory training for audit and other key financial efforts, and meet the legal requirement to achieve full audit readiness for all DoD financial statements by 2017."[15]

DoD is "responsible for establishing, maintaining and assessing internal controls to provide reasonable assurance that it meets the requirements of the Federal Managers' Financial Integrity Act" and by complying with OMB Circular No. A-123, "Management's Responsibility for Internal Control

7) Ibid.
8) Brook, D., (2001). Audited Financial Statements: Getting and Sustaining "Clean" Opinions, p. 34.
9) GAO-11-864T (2011). *DoD Financial Management: Numerous Challenges Must Be Addressed to Achieve Auditability,* p. 10
10) Ibid.
11) Hanks, C., (2009). Financial Accountability at the DoD: Reviewing the Bidding, p. 187.
12) Ibid, p. 190.
13) Ibid., pp. 184 & 192.
14) Brook, D., (2001). Audited Financial Statements: Getting and Sustaining "Clean" Opinions, pp. 29-30.
15) Panetta, L. (2011). Improving Financial Information and Achieving Audit Readiness Memo, pp. 1-2.

in the Federal Government."[16] DoD management uses certain criteria for identifying material weaknesses. These include meriting the attention of the resident and Congress, impairing essential operations or mission completion, or either noncompliance or nonconformance with laws and regulations or system requirements.[17] As stated previously, DoD has identified at least 13 uncorrected material weaknesses but does not have a comprehensive plan to address them.[18]

Another factor to achieving audit readiness is for DoD leaders to ensure that personnel are equipped with the knowledge, skills and abilities necessary for attaining that objective. However, GAO reported that DoD had not completed a "competency gap assessment in the existing or projected overall civilian workforce" or a "plan of action identifying recruiting and retention goals."[19] These were initially required by the National Defense Authorization Act for Fiscal Year 2006 and made a permanent requirement in the Fiscal Year 2010 Act.[20]

One of the most important factors to achieving audit readiness is for DoD leaders to ensure that personnel are held accountable for achieving audit readiness as part of their responsibilities. DoD had created a chief management officer position in response to limitations in "management responsibility, accountability and control over business transformation-related activities and applicable resources."[21] It wasn't until recently that audit readiness goals were part of evaluating the performance of senior executives. Limited oversight and accountability could slow the progression towards audit readiness.[22]

GAO has reported that DoD has updated its "corporate enterprise architecture," but it hasn't expanded that effort by adding "complete, coherent subsidiary architectures" for the individual DoD components.[23] In addition, GAO found that DoD did not have adequate policies and procedures for making investment decisions to address information technology and system requirements.[24] Therefore, DoD is missing a complete, well-defined architecture.

DoD personnel indicated that enterprise resource planning systems implementation is key to achieving the audit readiness milestone of Sept. 30, 2017. However, GAO found issues with the "Army's and Air Force's new general ledger system."[25] The issues included "operational problems, gaps in capabilities that required work-arounds and training that was not focused on system operation."[26] Therefore, DoD needs to lessen the delays in implementing these systems and ensure that the implementations are done correctly.

IDENTIFICATION AND ANALYSIS OF ALTERNATIVES

THE ALTERNATIVES

The alternatives and recommended solutions as identified by GAO and other research are listed below:

Alternative A— Maintain the Status Quo
Alternative B— Effective Plan to Correct Internal Control Weaknesses
Alternative C— Educated Financial Management Workforce
Alternative D— Accountability and Effective Oversight
Alternative E— Well-defined Enterprise Architecture
Alternative F— Successful Implementation of the Enterprise Resource Planning Systems
Alternative G— All of the Above Except Alternative A

ALTERNATIVE A: MAINTAIN THE STATUS QUO

DoD can continue on the current path, where "pervasive deficiencies in financial management processes, systems and controls, and the resulting lack of data reliability impair management's ability to assess the resources needed for DoD operations; track and control costs; ensure basic accountability; anticipate future costs; measure performance; maintain funds control; and reduce the risk of loss

16) Department of Defense Agency Financial Report for FY 2010, p. 30.
17) Ibid.
18) GAO-11-864T (2011). *DoD Financial Management: Numerous Challenges Must Be Addressed to Achieve Auditability,* p. 11.
19) GAO-11-827T (2011). DoD Civilian Personnel:*Competency Gap Analyses and Other Actions Needed to Enhance DoD's Strategic Workforce Plans*, p. 1.
20) House Armed Services Committee Panel on Defense Financial Management and Auditability Reform, Findings and Recommendations, January 24, 2012, p. 17.
21) GAO-11-181R (2011). *Defense Business Transformation: DoD Needs to Take Additional Actions to Further Define Key Management Roles, Develop Measurable Goals, and Align Planning Efforts,* p. 1.
22) GAO-11-864T (2011). *DoD Financial Management: Numerous Challenges Must Be Addressed to Achieve Auditability* pp. 12-13.
23) GAO-12-642T (2012). DoD Financial Management: *Challenges in Attaining Audit Readiness and Improving Business Processes and Systems,* p. 1.
24) Ibid. p. 19.
25) GAO-12-642T (2012). *DoD Financial Management: Challenges in Attaining Audit Readiness and Improving Business Processes and Systems,* p. 1.
26) Ibid.

from fraud, waste and abuse."[27] The current path would likely result in a disclaimer of opinion, and senior leaders would struggle to make major budgetary decisions using unreliable information.

ALTERNATIVE B: CORRECT MATERIAL WEAKNESSES

GAO indicated that "DoD currently has efforts underway to address known internal control weaknesses through three interrelated programs: (1) Internal Controls over Financial Reporting, (2) Enterprise Resource Planning Systems implementation and (3) the FIAR Plan."[28] However, DoD has not identified "specific control actions" for addressing all elements of the FIAR Plan, specifically those identified in Waves 4 and 5. GAO reported that those actions pertaining to "asset accountability and other financial reporting matters" need to be identified. GAO concluded that a "comprehensive plan that identifies all of DoD's internal control weaknesses would be critical to resolving long-standing weaknesses and will require consistent management oversight and monitoring for it to be successful."[29] As mentioned previously, Secretary Panetta has also emphasized addressing the internal control issue by requiring the execution of a full review of DoD's financial controls in the next two years and establishing interim goals to assess progress.

DoD IG testified that DoD's poor internal controls put it at risk of violating the Ant-Deficiency Act. Control environment weaknesses impair DoD's ability to "determine the amount of funds available to spend," leading to "potential over-obligating and over-expending appropriations." DoD IG reported that this condition was due to a lack of internal controls and training. GAO reached a similar conclusion.[30]

ALTERNATIVE C: EDUCATED FINANCIAL MANAGEMENT WORKFORCE

"Effective financial management in DoD will require a knowledgeable and skilled workforce that includes personnel who are trained and certified in accounting, versed in government accounting practices and standards, and experienced in information technology."[31] DoD has partially addressed this need by sending "almost 1,000 DoD personnel to professional development training that will assist them and their components in achieving the FIAR goal of auditable financial statements and to sustain audit readiness through effective internal controls." The curriculum was to enhance "knowledge and understanding of the FIAR goals and priorities." In addition, the fiscal year 2012 National Defense Authorization Act addresses the establishment of a "DoD Financial Management Certification Program for DoD's financial management workforce."[32] The goals of this effort are to—

- "Advance the professionalism of the DoD financial management workforce.
- Strengthen public confidence in DoD financial management by improving the financial management workforce's capabilities in audit readiness and analytics.
- Broaden the competencies and experience of the financial management workforce of other DoD business operations."[33]

The DoD Financial Management Certification Program is presumed to be a major force for "achieving and sustaining the DoD's FIAR goal of auditable financial statements by increasing the competencies and capabilities of the financial management workforce."[34] Secretary Panetta also required the implementation of a pilot certification program for financial managers in his Oct. 13, 2011, memo.[35] In

27) GAO-11-864T (2011). *DoD Financial Management: Numerous Challenges Must Be Addressed to Achieve Auditability,* p. 1.
28) Ibid., p. 11.
29) Ibid.
30) House Armed Services Committee Panel on Defense Financial Management and Auditability Reform, Findings and Recommendations, January 24, 2012, p. 21.
31) GAO-11-864T (2011). *DoD Financial Management: Numerous Challenges Must Be Addressed to Achieve Auditability,* p. 11.
32) Financial Improvement and Audit Readiness (FIAR) Plan Status Report (2011) for November, p. II-8.
33) Ibid., pp. II-8 & 9.
34) Ibid
35) Panetta, L. (2011). Improving Financial Information and Achieving Audit Readiness Memo, pp. 1-2.

addition, political scientist Paul C. Light has suggested a "capacity-based accountability" by "building organizations that are staffed, trained, structured and equipped to be effective" and advocated for "organizational competence."[36]

DoD IG has also embarked on a similar measure by upgrading and reemphasizing its internal certification programs, notably its Certified Defense Financial Auditor designation.[37] The Army Comptroller CP-11 Program is an example of a Service Agency's dedication to improving financial management and shares an emphasis in acquiring professional certifications and master's degrees, as well as gaining experience through developmental assignments.[38] By broadening their knowledge and experiences, DoD personnel will be able to solve complex issues directly or indirectly linked to audit readiness regardless of their expertise.

After developing these skill sets, DoD IG auditors and DoD financial managers may find ways to resolve issues without impairing independence. Agencies "with positive working partnerships between financial managers and auditors have achieved more clean audit opinions."[39] Collaborative arrangements such as "joint meetings throughout the year, defining problems and proposing solutions, interim reviews and negotiated agreements" were cited as possible examples.[40] In addition, "auditor independence is not impaired when offering routine advice or answering technical questions."[41] Perhaps, short-term line item, management controls or financial-related performance audits could be considered.

In addition, agencies "with positive cooperative arrangements between financial and line and functional managers have achieved more clean audit opinions."[42] Therefore, by implementing the DoD certification program, DoD financial and nonfinancial managers will become knowledgeable of everyone's role in achieving audit readiness.

ALTERNATIVE D: ACCOUNTABILITY AND EFFECTIVE OVERSIGHT

DoD "established a governance structure for the FIAR Plan, which includes review bodies for governance and oversight. To monitor progress and hold individuals accountable for progress, DoD managers and oversight bodies need reliable, valid, meaningful metrics to measure performance and the results of corrective actions."[43] GAO stated that "effective oversight holds individuals accountable for carrying out their responsibilities." DoD has taken steps by introducing incentives "such as including FIAR goals in Senior Executive Service Performance Plans." A second incentive entails "increased reprogramming thresholds granted to components that receive a positive audit opinion on their Statement of Budgetary Resources." A third incentive involves the funding of audit costs "by the Office of the Secretary of Defense after a successful audit." A final incentive is "publicizing and rewarding components for successful audits." The question now is whether the current metrics are sufficient in achieving meaningful results.[44]

"Agencies with the most reporting entities tend to have the fewest clean audit opinions." "The CFO Act does not require audits of reporting entity financial statements," but many agencies do require the independent audit of their respective reporting agencies' financial statements. DoD had twenty-six reporting entities.[45] The DoD could consolidate some of the reporting entities to simplify the reporting process. "CFOs with oversight of core financial management functions have more clean opinions than other CFOs." CFOs should have authority over "budget formulation, and execution, financial operations and analysis, and financial systems to comply with the CFO Act." "CFOs should not have additional responsibilities that distract them from financial management, such as agencywide information resource management, personnel, procurement, grants management and agency administration."[46] It appears that the DoD comptroller does have control over the three main financial management functions and not over "dis-

36) Light, P., (1993). *Monitoring Government Inspectors General and the Search for Accountability*. Washington, DC: The Brookings Institution, p. 3.
37) Department of Defense Inspector General's Certified Defense Financial Auditor Program and Audit Career Path (2011), p. 1.
38) Army Comptroller (CP-11) Program Handbook (2009). Retrieved April 12, 2012, at http://asafm.army.mil, pp. 1-1 to 4-3.
39) Brook, D., (2001). Audited Financial Statements: Getting and Sustaining "Clean" Opinions, p. 32,
40) Ibid.
41) Knubel, J., (2011). The CFO Act Financial Audit Process: A Unique Tool in DoD's Efficiency Toolbox. *The Journal of the American Society of Military Comptrollers*, Vol. 57, No. 32, p. 35.
42) Brook, D., (2001). Audited Financial Statements: Getting and Sustaining "Clean" Opinions, p. 32.
43) GAO-11-864T (2011). DoD Financial Management: Numerous Challenges Must Be Addressed to Achieve Auditability, p. 12.
44) Ibid., pp. 12-13.
45) Brook, D., (2001). Audited Financial Statements: Getting and Sustaining "Clean" Opinions, p. 27.
46) Ibid., p. 28.

tracting" functions. Therefore, these responsibilities should not be an issue.

ALTERNATIVE E: WELL-DEFINED ENTERPRISE ARCHITECTURE

GAO has continually designated DoD's business systems modernization program as high risk since 1995. Between 2001 and 2005, GAO reported that the "modernization program had spent hundreds of millions of dollars on an enterprise architecture and investment management structures that had limited value." Congress passed the Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005 that was consistent with GAO recommendations regarding the issue. In addition, the military departments' architecture programs continue to have scope and completeness limitations and maturity issues. GAO indicated these departments still lack a "fully-developed enterprise architecture methodology or a well-defined business enterprise architecture and transition plan to guide and constrain business transformation initiatives." Furthermore, the "DoD enterprise and the military departments' approaches to business systems investment management" are missing "the policies and procedures for effective investment selection, control and evaluation" methodologies. This alternative would mandate implementation of modernization controls.[47]

"GAO has continually designated DoD's business systems modernization program as high risk since 1995."

In addition, "agencies that made positive resource allocations to the effort have achieved more clean audit opinions." The Brook Study found that the two most important components are "positive application of personnel and money and insulating financial management from the effects of downsizing and resource constraints." Business-process improvements were noted due to the reassignment of staff "from lower priority duties to work on the financial statements."[48] In his Oct. 13, 2011, memo, Secretary Panetta directed the DoD comptroller to provide a plan to include resourcing the efforts to meet the goals.[49]

ALTERNATIVE F: SUCCESSFUL IMPLEMENTATION OF THE ENTERPRISE RESOURCE PLANNING SYSTEMS

DoD has invested "billions of dollars and will continue to invest billions more to implement the Enterprise Resource Planning System." DoD personnel have acknowledged that the ERPS are essential in "transforming DoD business operations, including financial management, and in improving DoD's capability for providing management and Congress with accurate and reliable information" as it pertains to the agency's operations. These ERPS are to "replace over 500 legacy systems," and therefore will address other operational weaknesses in DoD and would also produce savings. GAO reported that DoD "has not effectively employed acquisition management controls" to ensure that the ERPS deliver the expected capabilities on schedule and within budget. Delays in implementing the ERPS would extend the use and funding of duplicative systems, which would then decrease potential savings that could be applied more effectively elsewhere.[50]

"Agencies with the most financial management systems have the fewest clean audit opinions."[51] Thus, the importance of reducing the outdated systems can be linked to a "clean" audit opinion. In addition, "many agencies achieved clean opinions by employing short-term, "work-around" systems solutions."[52] DoD leaders could build a temporary, separate financial information system that would serve only the information needs of financial statements until the fully integrated system is operational. This may be viable as ERPS are expensive and subject to improvement. Objective: To determine whether any Railroad Medicare providers fraudulently billed for emergency transportation to routine dialysis or physical therapy appointments.

47) GAO-11-864T (2011). DoD Financial Management: Numerous Challenges Must Be Addressed to Achieve Auditability, pp. 13-4.

48) Brook, D., (2001). Audited Financial Statements: Getting and Sustaining "Clean" Opinions, p. 31.
49) Panetta, L. (2011). Improving Financial Information and Achieving Audit Readiness Memo, p. 1.
50) GAO-11-864T (2011). *DoD Financial Management: Numerous Challenges Must Be Addressed to AchieveAuditability*, pp.14-5.
51) Brook, D., (2001). Audited Financial Statements: Getting and Sustaining "Clean" Opinions, p. 26.
52) Ibid., p. 33.

ALTERNATIVE G: COMBINATION OF ALTERNATIVES B THROUGH F

Each issue identified as an alternative under Alternatives B through F represents one part of the solution. Therefore, DoD should implement Alternatives B through F to achieve audit readiness as noted by GAO.[53] Assuming a committed leadership is in place, DoD personnel need to address the problems pertaining to—

- Developing an "effective plan to correct internal control weaknesses."
- Ensuring an educated "financial management workforce."
- Ensuring "accountability and effective oversight."
- Ensuring a "well-defined enterprise architecture."
- Ensuring the "successful implementation of the enterprise resource planning systems."[54]

Therefore, DoD should improve its management control program by developing an effective plan to correct the identified weaknesses. DoD needs to ensure that its financial and nonfinancial managers are adequately trained as to what senior leadership's expectations are, as well as how the managers' efforts contribute to audit readiness success. DoD senior leaders should hold personnel accountable for achieving audit readiness and establish and maintain effective oversight so that milestones are not missed. DoD management should improve upon its enterprise architecture policies and give extensive consideration to ERPS implementation.

RECOMMENDED APPROACH

Best Alternative: G (Combination)

After considering GAO's and Congress' recommendations, as well as the Brook and Wiese Studies, and weighing all of the alternatives and outcomes, it was determined that Alternative G was the best choice. It minimized the differences among the trade-offs and minimized the opportunity costs. Under the shared assumptions that leadership commitment is the driving force, we can then conclude that the other alternatives (with the exception of Alternative A) would be practical.

IMPLEMENTATION STRATEGY

Assuming DoD has a committed and sustained leadership in place, DoD then needs to establish effective oversight and accountability. Accountability and oversight should be relatively easy to implement, and DoD has already established a governance structure for the Financial Improvement Audit Readiness Plan. However, GAO found that the senior governance officials, including the designated senior executive committees, were ineffective and inadequate.[55] Therefore, DoD leaders need to make the effort necessary to meet their audit readiness responsibilities. Implementing policies and procedures requires the support of DoD leaders to enforce corrective actions. Updates to the systems would require additional funding for implementation.

DoD should develop a comprehensive corrective action plan to address its material weaknesses. Timelines for implementing effective controls should be reported in future FIAR Plan status reports. Then, DoD leaders should allocate resources, whether it is for staff, funds, making system modifications, performing analyses, reevaluating methodologies or improving processes and procedures to correct the material weaknesses.

DoD leaders will then need to establish department committees with responsibility and accountability for the enterprise architecture. They need to ensure that methodologies, plans and procedures for making architectural and investment decisions are thoroughly defined and detailed.[56]

DoD leaders will need to assess the critical skills and competencies of the existing civilian workforce, the future critical skills and competencies desired over the next decade, and identifying the gaps under each assessment. Then, senior leaders should budget for hiring, training and continually educating the staff on financial management matters. DoD is already implementing a certification program similar to the one used for the acquisition workforce, and it establishes various competency levels. It is also exploring an exchange program with the private sector. Best practices and competencies will be shared.[57]

53) GAO-11-864T (2011). *DoD Financial Management: Numerous Challenges Must Be Addressed to Achieve Auditability,* p. 1.
54) GAO-11-864T (2011). *DoD Financial Management: Numerous Challenges Must Be Addressed to Achieve Auditability,* p. 1.
55) GAO-11-851 (2011). *DoD Financial Management: Improvement Needed in DoD Components' Implementation of Audit Readiness Efforts,*, pp. 1 & 25 and House Armed Services Committee Panel on Defense Financial Management and Auditability Reform, Findings and Recommendations, January 24, 2012, p. 17.
56) GAO-11-864T (2011). *DoD Financial Management: Numerous Challenges Must Be Addressed to Achieve Auditability*, p. 14.
57) House Armed Services Committee Panel on Defense Financial Management and Auditability Reform, Findings and Recommendations, January 24, 2012, p. 31.

After leadership involvement, oversight, a plan for correcting material weaknesses, enterprise architectural policies and training programs have been implemented, DoD senior leaders need to address the system side by developing or modifying ERPS to improve the output of reliable and accurate information. It appears that history has indicated several ERPS have not followed practical project management principles because their capabilities may not be on time or within budget. These include the Army's General Fund Enterprise Business System and the Air Force's Expeditionary Combat Support System, which have encountered delays and increased costs.[58] The outdated systems that the ERPS were to replace are still being utilized and funded. DoD IG renders the ERPS' effectiveness as questionable.[59] Therefore, the DoD should ensure that it is getting its "bang for its buck" by taking a harder look at the processes and procedures for developing and funding its ERPS requirements. The House Armed Services Committee Panel on DoD's Audit Readiness recommended that DoD assess even its "decision-making process regarding ERPS requirements at every level of authority."[60] Implementation would not be easy. However, DoD could implement temporary "work-arounds" to comply with Panetta's new mandated deadlines.

To implement this strategy, DoD leaders should consider the recommendations of Congress and GAO. Each step of this process involves various degrees of ease in implementing them. Since the previous and current secretaries of defense have responded to the growing political demands of improving DoD's financial management by taking some action, we should then expect that these efforts would assist in expediting DoD's readiness goals.

CONCLUSION

DoD has struggled since the implementation of the CFO Act to achieve audit readiness. Some have argued that either the accounting policies of McNamara's Pentagon, the lack of leadership commitment, the number of systems, missing competencies or awareness, the number of material weaknesses and other issues have been the causes for this dilemma. In addition, even if DoD achieves auditability, the battle is not over. In some ways, it has just begun. After becoming auditable and obtaining an opinion on its financial statements, DoD needs to be in a position to sustain that opinion. DoD may not achieve the unqualified "clean" audit opinion the first go round, since a qualified opinion is also likely. Nevertheless, by implementing the proposed solution, which is supported by both Congress and GAO, DoD should achieve audit readiness. However, it's still too early to tell whether sustaining an opinion and obtaining a clean opinion are viable.

DoD, GAO, DoD IG and other observers and stakeholders have published a plethora of literature that addresses either specifically or contextually the importance of DoD's audit readiness. DoD has issued its FIAR Plan as a road map to achieving auditability. The GAO and DoD IG have addressed what they see as stumbling blocks to that goal. Congress has taken interest and wants to ensure that the DoD stays focused in its efforts. Further investigation should be considered in determining the costs involved in meeting those requirements, so that a fair cost-benefit analysis can be done. Also, how does DoD compare to some of the largest corporations in America? The legendary Greek mathematician Pythagoras, known for his theorem of triangles, believed that the world's problems could be solved with numbers.[61] Can the same be said for DoD? How can audit readiness help improve the current budget crisis? Initially, as I considered alternatives to the status quo, my thought was to determine how DoD would achieve other opinions on its financial statements assuming that the current disclaimer wasn't feasible and the ideal unqualified opinion wasn't reachable. However, after concluding my research, I determined that evaluating the agreed-upon solutions to achieving audit readiness first, rather than the ultimate goal of a clean opinion, may be the more reasonable approach.

58) Ibid., pp. 34-9.
59) Ibid., p. 18.
60) Ibid. p. 44.

61) Huffman, Carl, "Pythagoras", *The Stanford Encyclopedia of Philosophy (Fall 2011 Edition)*, Edward N. Zalta (ed.), URL = http://plato.stanford.edu/archives/fall2011/entries/pythagoras/. Retrieved April 16, 2012, p. 1.

James Davis Jr.

James B. Davis, Jr, is a senior auditor/team leader with auditing at the Department of Defense Inspector General. At DoD IG, Davis is primarily assigned to civilian payroll and military retirement fund engagements. He has also worked on the DoD-wide financial statement audit and performed background work for the Iraq/Afghanistan Security Forces Fund engagement. Davis is a certified defense financial auditor (Level III) and has served on the employee council. He has also served as an agency recruiter and as a mentor in the DoD IG Mentorship Program.

Prior to his employment at DoD IG, Davis was a staff auditor for the Army Audit Agency where he worked on Base realignment & closure, management controls, Army Corps of Engineers, headquarters Department of the Army service contract, Army privatization workload, post most efficient oganization decision, and Army Financial Statements engagements. While at the Army Audit Agency, he co-chaired the 2001 Combined Federal Campaign for the National Capital Region, which brought the agency the President's Award and Pacesetter Award.

Prior to his employment at the Army Audit Agency, Davis worked for the West Virginia Department of Tax and Revenue as a revenue agent and later as a tax auditor. In these positions, he reviewed the records and tax returns of businesses in West Virginia and neighboring states to ensure compliance with West Virginia tax laws. He also advised taxpayers on tax policy. Prior to that, Davis was employed as a controller for several area small businesses.

He is a certified public accountant, licensed in both West Virginia and Virginia. Davis is also a certified government financial manager and is a member of the Northern Virginia Chapter of the Association of Government Accountants, where he has held regional and chapter offices in AGA and served on the AGA National Early Careers Task Force. He is the recipient of several AGA national, regional and chapter awards, including AGA's National Community Service Award, AGA's National Chapter CGFM Award and the AGA Capital Region Regional Vice President's Award. In addition, Davis is a certified defense financial manager and has either chaired or co-chaired committees for the Mount Vernon Chapter of the American Society of Military Comptrollers that have received national recognition. He is also a certified fraud examiner and is a member of the Association of Certified Fraud Examiners. Davis has chaired the Government Relations Committee of the Northern Virginia Chapter of the Institute of Internal Auditors and had served on the 2002 IIA International Conference Host Committee. Furthermore, he is a member of the Delta Sigma Pi Professional Business Fraternity and served on the Host Committee for the 2009 Grand Chapter Congress. Davis is a member of the Young Government Leaders organization. He received a Bachelor of Science in accounting from West Liberty State College, now West Liberty University. Davis recently earned a Master of Policy Management from the Georgetown University Public Policy Institute, and this article is an excerpt from his capstone paper.

Inspectors General Auditing Strategies for Federal Executive Branch Agencies in Light of Unfunded Mandates

By Loralee Bennett

An unfunded mandate is generally defined as a law passed by the federal government that requires states, local governments or nongovernmental agencies to perform an action for which the federal government has provided no money to take the required action.[1] Congress, recognizing this was a problem, passed the Unfunded Mandates Reform Act of 1995 to "curb the practice of imposing unfunded federal mandates on states and local governments."[2] However, prior to passage of the UMR Act, there was a more expansive definition of an unfunded mandate. Specifically, an unfunded mandate referred "to a requirement that a unit of government imposes without providing funds to pay for costs of compliance."[3] However, with the more limited definition that has come to prominence since the passage of the UMR Act, there is an often forgotten recipient of unfunded congressional mandates once covered under the definition—federal executive branch agencies.

1) Wise Geek. (1995). Wise Geek. Retrieved October 13, 2011, from Unfunded Mandate: http://www.wisegeek.com/what-is-an-unfunded-mandate.htm.
2) Congress. (1995, March 22). Public Law 104. Retrieved October 13, 2011, from Government Printing Office: http://www.gpo.gov/fdsys/pkg/PLAW-104publ4/pdf/PLAW-104publ4.pdf.
3) Bea, K., & Beth, R. S. (2005). Unfunded Mandates Reform Act Summarized (RS20058). Washington DC: Congressional Research Service.

While Congress passes a wide range of laws, these laws are "primarily aimed at changing government programs and agency policies and practices."[4] While such programs can be administered by non-federal entities, for example state governments, these programs are most often administered by federal executive branch agencies. Additionally, congressional changes to agency policies and procedures are usually those of federal executive branch agencies.

"However, with the more limited definition that has come to prominence since the passage of the UMR Act, there is an often forgotten recipient of unfunded congressional mandates once covered under the definition—federal executive branch agencies."

When it comes to funding federal agencies and/or federal programs established in law and executed by federal executive branch agencies, there is a two-step process. First, an authorization is passed that establishes either the agency or the federal program. The authorization outlines the aim of the program and sets policies that agencies must follow during implementation. Additionally, the authorization establishes a funding ceiling for the program. The authorization, however, does not actually provide the funding. For funding, we move

4) Haskell, J. (2010). Congress in Context. Jackson: Westview Press.

to the second step, an appropriation. An appropriation, when passed, actually provides the funding for the agency and/or program for the given fiscal year. The appropriation, however, is rarely as high as the funding ceiling established in the authorization.[5]

"...the federal deficit is so large, that the only alternative left for imposing so-called national solutions is to impose unfunded mandates."

While the funding may be less than the authorized ceiling, in a perfect world the appropriation would provide the agency with sufficient funding to adequately implement or administer the program established in law. However, the appropriation is generally set based on budgetary constraints and not necessarily on the needs of the program. Therefore, funding levels can fall well below the actual amount necessary to properly implement or run a program or to achieve all of the program's aims. In fact, Senator Kempthorne was quoted as stating, "[t]he federal government no longer has the money to fund the governmental actions it wishes to see accomplished throughout the country. In fact, it has not had the money to do this for many years. Instead, it borrowed for a long time, to cover those costs. But now the federal deficit is so large, that the only alternative left for imposing so-called national solutions is to impose unfunded mandates."[6] Despite the lack of funding from Congress, federal executive branch agencies are still required, by law, to implement the programs passed by Congress.

To ensure federal executive branch agencies implement the programs it passes, Congress passed the Inspector General Act (as amended), which established an office of inspector general in most federal executive branch departments and agencies. The purpose of the IG Act was to create independent and objective units to (1) conduct and supervise audits and investigations, (2) recommend policies to improve operations and prevent fraud and (3) to keep the leadership and Congress informed of problems and their associated corrective recommendations. The IG Act goes on to state that it is the duty of each inspector general to (1) provide policy direction, (2) review existing and proposed legislation and inform Congress of the impact of such legislation on the agency, (3) promote economy and efficiency and (4) keep the department and/or agency head and Congress fully informed of problems.

Paul Light[7] points out that, to comply with the IG Act, inspectors general rely heavily on compliance accountability. However, there are actually three possible approaches to accountability in government. "The first approach, compliance accountability, rests on efforts to assure conformity with carefully drawn rules and regulations. Using negative sanctions targeted primarily at individuals inside or outside (for example, contracts and beneficiaries) of government, compliance accountability places its faith in correcting problems after they occur and in the deterrence value of visible punishment. The second approach, performance accountability, centers on the establishment of incentives and rewards for desired outcomes. Using positive sanctions, again targeted primarily at individuals, performance accountability puts its emphasis on moving individuals toward the preferred results from the beginning. The third approach, capacity-based accountability, involves the creation of organizational competence through technologies—people, systems and structures—and the

5) Ibid.
6) Dilger, R., & Beth, R. (2011). Unfunded Mandates Reform Act: History, Impact, and Issues (R40957). Washington DC: Congressional Research Service.
7) Light, P. C. (1993). Monitoring Government: Inspectors General and the Search for Accountability. Washington: The Brookings Institute and The Governance Institute.

maintenance of the conditions of success through initial investment. With the availability of adequate resources, capacity building focuses on building organizations that are staffed, trained, structured and equipped to be effective."[8]

In short, compliance accountability looks for errors that have already occurred and focuses on correcting those problems. Performance accountability (or economy and efficiency reviews) is designed to help agencies perform their mission in the most economical manner possible. Put another way, they help the agency meet mission requirements while using less resources. Capacity-based accountability helps new agencies "come on line" with the most effective and efficient organizational operation from the very beginning.

While the IG Act allows for all three types of reviews, most inspectors general rely "almost exclusively on compliance" reviews.[9] A review of the mission statements of several of the larger inspectors general supports Light's assertion. The mission statements focus on oversight from the standpoint of compliance types of reviews versus a focus on performance accountability or capacity-based accountability (as defined by Light). For example, a review of the Department of the Treasury's inspector general website disclosed that the inspector general's focus is on keeping "both the Secretary and the Congress fully informed about the problems and deficiencies relating to the administration of the department programs and operations and the necessity for corrective action."[10]

This highly-focused compliance viewpoint is understandable. Inspectors general had that outlook almost from the beginning. Specifically, looking back at the history of inspectors general, we see the same limitation. Most reviews focused on compliance monitoring. In fact, "in one of the first resolutions passed, the Continental Congress established an IG, concluding that it was essential to the promotion of discipline in the American Army, and to the reformation of the various abuses which prevail in the different departments."[11] Essentially, inspectors general were established because of scandals surrounding the Colonial army and their focus was on ensuring compliance with governing policy.

Another reason inspectors general tend to focus on compliance reviews is because "compliance monitoring yields more attractive results politically." "Compliance monitoring not only generates a much greater volume of findings of failure, and therefore higher visibility, … but also produces recommendations for actions that are less expensive, more politically palatable, cleaner jurisdictionally, and faster to implement."[12] As Schwartz so aptly stated, "justly or unjustly, time spent putting out visible fires gains one more credit than the same time spent sniffing for smoke."[13] Specifically, "a high degree of political consensus surrounds the simple goal of most compliance recommendations: to punish the cheaters and abusers."[14]

However, "compliance accountability places its faith in correcting problems after they occur and in the deterrence value of visible punishment."[15] In short, compliance reviews look at the program's adherence to regulatory or legal requirements and then reports on the success or failure of compliance

with those requirements. Additionally, following identification of any failures to comply with the requirements, the resulting Office of Inspector General report will contain recommendations, based on the cause of the noncompliance, identifying actions the agency should take to come into compliance with the requirements.

8) Ibid.
9) Ibid.
10) Treasury OIG. (2011, May 11). Inspector General. Retrieved October 16, 2011, from Department of the Treasury: http://www.treasury.gov/about/organizational-structure/ig/Pages/about.aspx.
11) Light, P. C. (1993). Monitoring Government: Inspectors General and the Search for Accountability. Washington: The Brookings Institute and The Governance Institute.
12) Ibid.
13) Schwartz, T. (1989). Checks, Balances, and Bureaucratic Usurpation of Congressional Power. In B. W. Grofman, The Federalist Papers and the New Institutionalism (pp. 150-157). New York: Agathon Press.
14) Light, P. C. (1993). Monitoring Government: Inspectors General and the Search for Accountability. Washington: The Brookings Institute and The Governance Institute.
15) Ibid.

When conducting a compliance-focused audit, inspection or evaluation of a federal executive branch agency that is designed to validate the agency's compliance with Congressional mandates passed in public laws, it has become more common to learn that the cause of noncompliance is because the agency simply lacks the staff, money or other resources necessary to comply with the requirement. Essentially, the problem exists due to an unfunded Congressional mandate. For example, a recent evaluation of a Bureau of Land Management Field Office examined annual oil and gas inspection and enforcement efforts. The evaluation disclosed that the Federal Oil and Gas Royalty Management Act of 1982 required BLM field offices to annually inspect all high-priority federal and Indian cases and 33 percent of low-priority cases. For the field office visited, implementation of FOGRMA meant that it was required to conduct 742 oil and gas inspection and enforcement activities for the year reviewed. However, the field office set their target for that year at only 542 activities—200 below the number required by FOGRMA. When questioned, field office management indicated this was because they simply did not have the staff to perform the number of activities FOGRMA required. Additionally, not only was the target set well below the number FOGRMA required, the field office was unable to even complete the targeted number of inspections because it did not have the staff necessary to complete the activities and did not have the money to hire more.

Responses from agency officials claiming noncompliance with program mandates as a result of an unfunded Congressional mandate

"With shrinking budgets in the federal arena, any potential solution to this quandary needs to acknowledge the fact that more resources are unlikely to be appropriated by Congress..."

makes determining what to review and/or what to recommend difficult for the inspectors general community. First, reviews conducted by an office of inspector general normally do not include a review of whether appropriate resources have been authorized or funded. Second, when noncompliance exists as a result of an unfunded Congressional mandate, recommendations to correct the problem are difficult to craft. Agencies generally already know they are noncompliant, but lack the resources necessary to comply with the Congressional mandate. In such cases, simply recommending they come into compliance will either not correct the problem because they lack the resources to come into compliance, or it forces the agency to divert resources from another program, thereby simply shifting the noncompliance problem from one program area to another. Both result are counterproductive and wasteful. However, an agency's noncompliance with laws or regulations is also unacceptable. As a result, the inspectors general community is faced with a quandary in these situations.

With shrinking budgets in the federal arena, any potential solution to this quandary needs to acknowledge the fact that more resources are unlikely to be appropriated by Congress—to either the inspectors general or the agencies they oversee. Despite a lack of additional resources, research identified five potential alternative solutions to this quandary: (1) As advocated by Light,16 inspectors general can begin conducting more performance reviews (helping agencies perform their mission in

16) Ibid.

the most economical manner possible) compared with compliance reviews (finding noncompliance with requirements after the fact); (2) Instead of moving away from compliance reviews, inspectors general can add a resource assessment component to compliance reviews, to assess the resources available compared to the resources required, when the cause of noncompliance is reported to be a lack of resources; (3) Like the state and local governments, the inspectors general community can begin lobbying Congress to have either federal executive branch agencies added to the UMR Act or a separate, but similar, act passed covering federal executive branch agencies; (4) Inspectors general can review existing and proposed legislation or regulations related to programs of the agencies they oversee and make recommendations in the Semi-Annual Report to Congress concerning the impact of such legislation or regulations on the administration of the programs; (5) As is always available, the inspectors general can also choose to do nothing to address the situations and live with them.

Once we identified the potential solutions, we created a matrix of the five alternatives and compared and evaluated each alternative against three different sets of criteria. Specifically, each alternative was evaluated against: (1) The three purposes of the IG Act. If the alternative did not meet all three purposes of the IG Act, it would have to be eliminated as an alternative since it would not be in compliance with the law. (2) The four responsibilities of the IG Act. If the alternative did not meet at least one responsibility of the IG Act, it would have to be eliminated as an alternative since it would not be in compliance with the law. (3) Five overall questions developed to identify the alternative with the highest probability of successful implementation.

"However annual funding amounts in appropriations are generally set based on budgetary constraints and not on the agency's or program's actual resource requirements necessary to implement the mandates or meet the goals."

Based on the matrix and the analysis conducted, the best alternative for implementation is the alternative to review existing and proposed legislation. Additionally, of all four of the alternatives that required change, this alternative is probably the least controversial and easiest to implement. This is because the alternative can be implemented inside just one component office inside an individual office of inspector general. As a result, significant resistance from staff uncomfortable with change is unlikely since very few individuals within the office of inspector general would be affected. Further, each office of inspector general can implement the alternative independent of the inspectors general community. While implementation of the alternative would benefit all inspectors general, the success or failure of implementation of the alternative in a given office of inspector general would not rely on cooperation across the inspectors general community. This would make successful implementation more feasible. Consequently, each Office of Inspector General should implement the alternative to review existing and proposed legislation affecting the programs, agencies and department they oversee.

Inspectors general should ensure, however, as part of reviewing existing and proposed legislation, that not only authorizations are reviewed but that annual appropriations are reviewed as well. Even those inspectors general who currently have procedures in place to review existing and proposed legislation focus their reviews on authorizations since authorizations outline the aim of the program and

"A problem—any problem—cannot be fixed if no one knows it exists."

sets policies that the agencies must follow, information necessary to evaluate an agencies compliance, or noncompliance, with a mandate. Therefore, authorizations are reviewed with an eye toward compliance reviews since, as we stated earlier, there appears to be significant support for a focus on compliance reviews from Congress and, inspectors general have gotten very good at conducting them. By ensuring that annual appropriations are reviewed, inspectors general can also provide Congress—in the Semi Annual Report to Congress—a simple and effective way to compare the level of funding thought to be required for the program or agency to operate successfully (identified in the authorization) and the actual level of funding provided to operate the program or agency (identified in the appropriation).

CONCLUSION

Annual funding in appropriations for agencies and programs are rarely as high as funding ceilings established in authorizations. When establishing a funding ceiling authorization, legislators should be reviewing the mandates and goals established for the agency or program in the authorization and then establishing a ceiling that only allows the mandates and goals to be met. In a perfect world, annual appropriations would then provide sufficient funding to adequately implement or administer the agency or program and ensure the agency's or program's mandates and goals, as established in law, were met. However, annual funding amounts in appropriations are generally set based on budgetary constraints and not on the agency's or program's actual resource requirements necessary to implement the mandates or meet the goals.

Alternatives, which allow the inspectors general community to help the agencies they oversee meet unfunded congressional mandates, are limited by the mandates that Congress has imposed on the inspectors general community itself.

However, a careful review of governing legislation disclosed a number of alternatives available to the inspectors general community, which had the potential to help agencies address the unfunded Congressional mandate problem. Based on the analysis conducted of the available alternatives, the best way for inspector general's offices to help the agencies they oversee is to review existing and proposed legislation that relates to the agencies it oversees and make recommendations in the Semi Annual Report to Congress concerning the impact of such legislation on the agency's resources—including funding—or its ability to administer the programs and meet mandates. This review should also include a comparison of each program's authorization compared to its annual appropriation.

While implementation of this alternative will not prevent Congress from imposing unfunded congressional mandates on federal executive branch agencies, passage of the UMR Act did not prevent Congress from imposing unfunded Congressional mandates on state and local governments either. Instead, implementation of this alternative will bring specific cases of unfunded congressional mandates on federal executive branch agencies to light. As a result, like the UMR Act exposed the problem related to state and local governments and resulted in a decrease of unfunded Congressional mandates on those institutions, exposing the problem related to federal executive branch agencies should result in a decrease in the number of unfunded congressional mandates imposed on these agencies.

A problem—any problem—cannot be fixed if no one knows it exists. Offices of Inspectors General have demonstrated a noteworthy ability to identify and expose problems. Implementation of an alternative to review existing and proposed legislation, identify cases of insufficient funding and notify Congress of problems identified plays directly into one of the major strengths of every Office of Inspector General. ☙

Loralee Bennett

Loralee Bennett graduated with honors from Utica College of Syracuse University in 1989 with a major in accounting. Upon graduation, she accepted a job with the Air Force Audit Agency at Lowry Air Force Base in Denver. When Lowry AFB made the Base Closure and Realignment Commission listing, she transferred to Elmendorf AFB in Anchorage, Alaska. Bennett made her way back to the Air Force Audit Agency at Wright-Patterson AFB in Dayton, Ohio, by way of Ramstein AFB, Germany. During her nine years with the Air Force Audit Agency, she performed both field-level audits and Air Force-wide program audits, earned a master's degree in administration from Central Michigan University and became a certified internal auditor.

In 2001, Bennett transferred to the Department of Agriculture's Office of Inspector General in Kansas City, Mo.

During her four years with Agriculture's IG office, Bennett performed financial and information technology audits. In 2006, she transferred again to the Department of the Interior's Office of Inspector General, accepting a position as the field office director over their Albuquerque, N.M., field office. During her time there, most projects she supervised were in Indian Country. From there, she was promoted to the Central Region deputy regional audit manager position in Denver, where she supervised as many as 30 projects at a time, while taking care of all personnel and administrative issues.

In 2010, Bennett was promoted to headquarters operations, her current position, where she works with all six regions to ensure projects are on time, schedule and budget. She is also responsible for completion of the annual audit plan and all internal training.

Council of the
INSPECTORS GENERAL
on INTEGRITY *and* EFFICIENCY

For information regarding the
Council of the Inspectors General
on Integrity and Efficiency
please contact:
phone: (202) 292-2600
email: cigie.information@cigie.gov

Inspector General Act of 1978, as amended Title 5, U.S. Code, Appendix

2. Purpose and establishment of Offices of Inspector General; departments and agencies involved

In order to create independent and objective units--

(1) to conduct and supervise audits and investigations relating to the programs and operations of the establishments listed in section 11(2);

(2) to provide leadership and coordination and recommend policies for activities designed (A) to promote economy, efficiency, and effectiveness in the administration of, and (B) to prevent and detect fraud and abuse in, such programs and operations; and

(3) to provide a means for keeping the head of the establishment and the Congress fully and currently informed about problems and deficiencies relating to the administration of such programs and operations and the necessity for and progress of corrective action;