

A SUPPLEMENT TO

SECURITY SYSTEMS NEWS

**SIA**

# FISCAL YEAR INFORMER

## ▶ **Tips for Success**

Selling to the Government, it's not for everyone **3**

## ▶ **Billions and Trillions**

Obama's Budget Proposal and Security **4**

## ▶ **Immigration Bill**

Billions for border security enhancements **8**

Q2 : 2013



# Security Technology

*Free*  
Webcast Series



**SECURITY SYSTEMS NEWS**

Hear from security experts on how new technologies will impact your business.

The Security Industry Association and Security Systems News present a webcast series that brings up-and-coming technology to the frontlines for security professionals.

*Registration  
is Free!*

**JUNE**  
**The Impact of NFC on Access Control**

**OCTOBER**  
**Wireless Development: 3G vs 4G & the 2G Sunset**

**SEPTEMBER**  
**BYOD: Security Liability & Policy**

**DECEMBER**  
**TechEV(olution): Keeping Up with Technology & the Bottom Line**

Register at: [securitysystemsnews.com/webcasts](http://securitysystemsnews.com/webcasts)

# TIPS for Success in the Federal Market

*Selling to the government is not for everyone. There are, however, some tried and true basics that can help you decide if it is right for you.*

**By: Kristina Tanasichuk**

## **Pull Up a Chair and Make Yourself Comfortable**

In most cases, it takes a laser focus, significant marketing and an 18-24 month commitment to make traction and build the partnerships necessary for success in the federal market. Although government opportunities are posted on [www.fedbizopps.com](http://www.fedbizopps.com), companies savvy about the workings of the federal market know that by the time these opportunities are posted, a great deal of marketing, relationship-building and resource expenditure has already taken place. A company turning to the government for a quick contract to boost revenue may be very disappointed. The good news is that, if you stay the course, the rewards are well worth it.

## **Where do I start?**

First, the Small Business Administration (SBA) has a series of free online courses to help you understand the basics of contracting at [www.sba.gov/gcclassroom](http://www.sba.gov/gcclassroom). Nearly all federal agencies have an Office of Small and Disadvantaged Business Utilization (OSDBU) and a procurement division. Getting to know these folks will help you navigate the agency and find the right people. A list of the federal OSDBUs and their roles is available at [www.osdbu.gov](http://www.osdbu.gov).

Ensuring that your internal capacity is adequate to execute and operate in the federal market is also critical. Contracting requires adherence to the Federal Acquisition Regulation (FAR), which includes specific accounting and billing procedures from the Defense Contract Audit Agency (DCAA), as well as other agency-specific requirements, such as security clearances and facilities standards. Thorough research on what you must build internally is as critical to your success as your efforts externally.

## **Small Business Set-Asides and Other Programs**

There are numerous programs designed to help small companies get started in the federal market: HUBZone, 8(a), Women-Owned Small Business (WOSB) and Service Disabled Veteran-Owned (SDVO) are a few examples. Learn more about the requirements of each at <http://www.gtscoalition.com/small-business-set-aside-program/>. The Small Business Innovation Research (SBIR) program helps companies develop products through research grants. Finally, a number of agencies have mentor-protégé programs that pair large, experienced contractors with small companies in the pursuit of federal opportunities.

## **Why You?**

The government market is extremely competitive – even more so with sequestration and budget cuts. Being able to articulate clearly your company's core competencies and market differen-

tiators is critical to making your case to potential federal clients and industry partners. Develop a capability statement that is succinct and demonstrates what you do and why your company is different from your competitors. This is your “elevator pitch” on paper.

## **Understand Your Customers and the Way They Buy**

Government customers are pulled in numerous directions. Their priorities and purchases are influenced by budgets controlled by Congress, political considerations, the FAR, and other programs that may have nothing to do with whether the customer wants to buy or not. Understanding their environment, challenges and needs is critical to your success.

## **Where's the Money?**

Now that you know your customer, where does their money come from, and is it coming at all? You can have the best idea, technology or product, but if the solution is not funded, or is not a priority, it will be difficult to get traction. Following the congressional budget process and determining whether certain programs or priorities are funded is critical. No money, no sale.

## **Plan Strategically**

Will you be the prime contractor or act as a subcontractor to a larger firm? Are you interested in further development of a product or technology? Is there the possibility of a sole source contract? (Are your competencies so unique that you are the only provider?) Weathering the federal market by yourself is tough; partners can help you create a comprehensive solution. Determine how your core competencies can contribute to a solution and whether your position is strongest alone or with a partner.

## **Network. Network. Network.**

Good grief! Where do you start to know agency priorities, congressional budgets, potential partners and all the regulations to which you must adhere? Maximize your reach by working with organizations that help you understand the market and build your contacts. Numerous non-profit organizations exist to help navigate the complex federal arena, and they provide the best way to get up to speed quickly. ■

*Kristina Tanasichuk (@GTSCoalition) is the founder and CEO of the Government Technology & Services Coalition, a non-profit organization founded by small and mid-sized CEOs to provide exceptional advocacy, capacity building, partnership opportunities and marketing in the federal homeland security and national security market. Visit us at [www.gtscoalition.com](http://www.gtscoalition.com).*



# Billions and Trillions: Obama's Budget Proposal and Security

By: **Kathleen Carroll**

If you were to count the individual dollars that the federal government spends every year, and you did so at the rate of one dollar per second, you would have demonstrated very poor hobby-selecting abilities.

But say an eccentric and wealthy fellow offered to pay you handsomely for the job and promised you a huge bonus upon completion. Working 40 hours a week for five days a week and taking two weeks of annual vacation, you could expect to get that big check in just 525,000 years.

According to the Office of Management and Budget – an agency that, we hope, does not have people on staff who count individual dollars, but we can't be sure – President Obama has proposed spending \$3.78 trillion in fiscal year 2014, which begins on Oct. 1. The federal government is expected to collect \$3.03 trillion in revenues in FY14, leaving a deficit of \$744 billion. Over the next 10 years, Obama projects that federal spending will total \$46.50 trillion, revenues \$41.23 trillion and combined deficit spending \$5.27 trillion.

The president's budget will not pass as written, but the total amount of spending next year will be pretty close to his figure, largely because automatically-funded entitlement programs such as Social Security, Medicare and Medicaid and interest payments on the \$16.8 trillion national debt – be glad you don't have to count that one – combine to account for about two-thirds of the budget. "Discretionary" spending – basically, the programs on which lawmakers and the president have to reach some sort of agreement in order for a budget to be enacted – is the remaining one-third. And about half of that is for defense.

Within that one-half of one-third – which is still quite a bit of money, of course – are many programs that relate to the security of public places. Obama wants to provide \$39 billion to the Department of Homeland Security next year, which includes \$4.8 billion for the Transportation Security Administration.

Projects that are funded at \$1 billion or less can almost be considered fiscally trivial – apologies to the late Everett Dirksen – yet they still often get a lot of attention in Congress and the media. Among the proposed security-related spending in this category is:

- \$810 million to support efforts to protect federal computer systems and networks from cyber attack, disruptions and exploitations; strengthen state and local governments' cybersecurity capacity; and support private sector efforts to protect critical infrastructure.

- \$494 million to fund research and development in cyber-security, explosives detection and chemical/biological response systems.
- \$114 million to enhance the E-Verify system by expanding system capacity, upgrading fraud prevention and detection capabilities, and improving individuals' ability to ensure that their employment eligibility records are accurate.

Obama's proposal also outlines a new approach to some security-related federal grants. Whereas money for ports, transit systems and other areas have been provided through their own programs, the administration wants to instead have a combined National Preparedness Grant Program, managed at the state level, to which it would provide \$2.1 billion in FY14.

"Using a competitive risk-based model, the National Preparedness Grant Program will apply a comprehensive process that identifies and prioritizes deployable capabilities, ensures grantees put funding to work more quickly, and requires grantees to regularly report progress in the acquisition and development of these capabilities," the budget proposal stated.

Some groups, including the Security Industry Association, have expressed concerns about this approach, with the American Association of Port Authorities (AAPA) President and CEO Kurt Nagle telling Congress that his organization would prefer to have the dedicated federal programs continue.

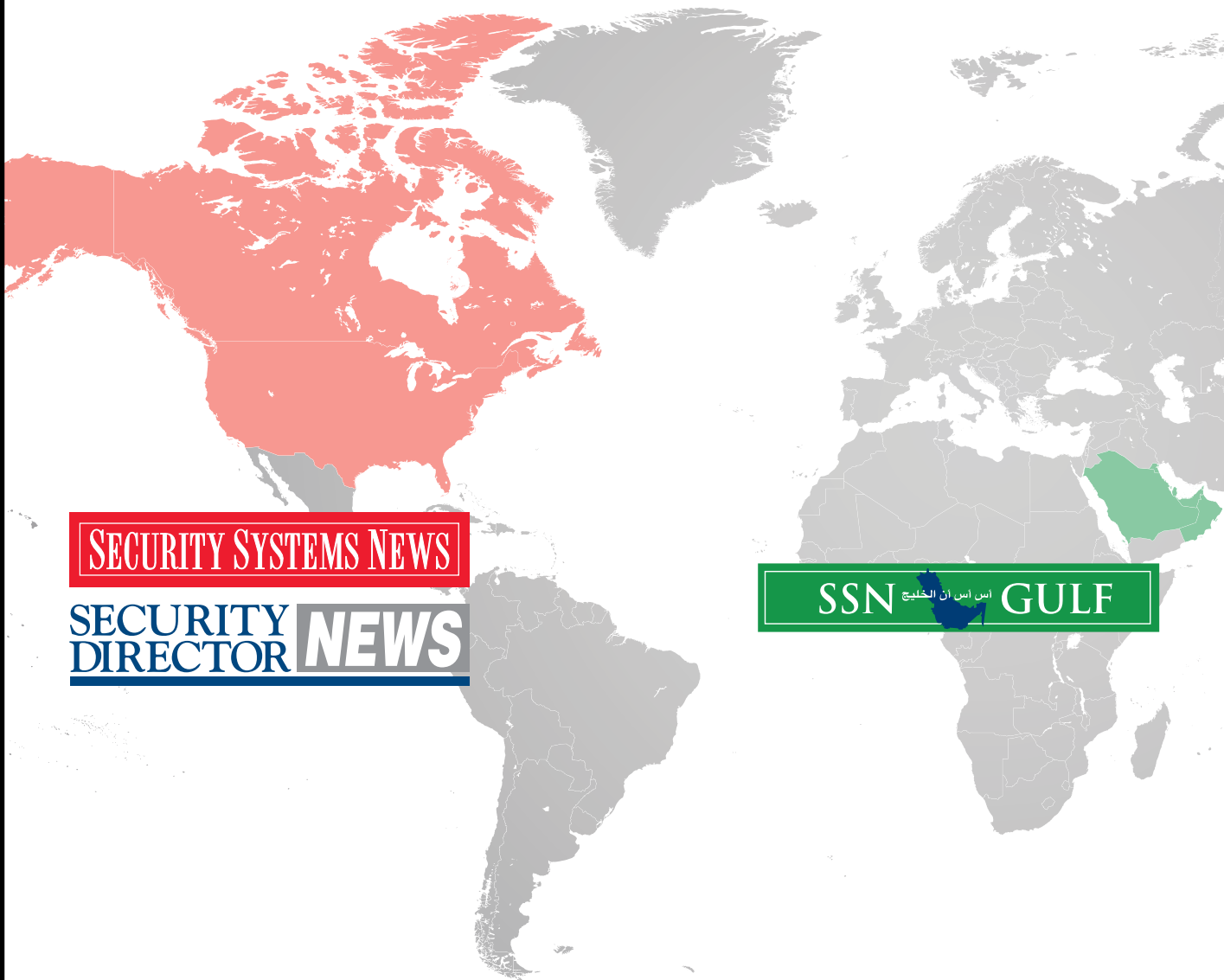
"State governments, while responsible for many important tasks, are not primarily focused on securing international borders," Nagle said at a March 13 hearing of a subcommittee of the House Homeland Security Committee. "If given discretion over how federal security grant monies should be spent, AAPA is concerned states will not prioritize seaport security, resulting in a distribution of funds not based on relevant standards for such decision-making."

Congressional Republicans will, of course, have their own ideas about how to fund these agencies and projects, and lots of debating and deal-making remains to be done. If all goes as scheduled, we'll know what the final spending numbers for FY14 are in late September. If all goes as expected, it will be much later. ■

*Kathleen Carroll is the director of government relations for HID Global. She also serves as the chairperson of the SIA Government Relations Committee. She can be reached at kcarroll@hidglobal.com.*



# Global Security News Coverage



**SECURITY SYSTEMS NEWS**

**SECURITY  
DIRECTOR NEWS**

**SSN** أس أس أن الخليج **GULF**

[www.SecuritySystemsNews.com](http://www.SecuritySystemsNews.com)

[www.SecurityDirectorNews.com](http://www.SecurityDirectorNews.com)

[www.SSNGulf.com](http://www.SSNGulf.com)

**For more information, contact:**

Tim Purpura

*Group Publisher*

[tpurpura@securitysystemsnews.com](mailto:tpurpura@securitysystemsnews.com)

# Department of Homeland Security – President’s Budget Request and the Appropriations Process

*By: Andrew Howell*

As spring turns to summer, congressional appropriations committees ramp up their activity on spending bills. Though the Obama administration delayed submitting its Fiscal Year 2014 Budget Request well beyond the traditional early February timeframe, the 12 subcommittees charged with developing spending bills are now working through their process, holding hearings and getting briefings from departments and agencies.

The House and Senate Homeland Security appropriations subcommittees are looking at a Department of Homeland Security (DHS) budget request that acknowledges that the trend of ever-increasing spending is over, and that the fiscal constraints that have dogged other departments now are taking hold.

The major DHS components (Customs and Border Protection (CBP), Coast Guard and the Transportation Security Administration (TSA)) are personnel-heavy, and those aspects of their budgets were spared the budget scalpel, and, in some cases, new fees may offset additional spending. In this tight budget environment, personnel expenses were prioritized over the acquisition of new technology and equipment. Some programs were stopped, others delayed. This means that additional funds must be dedicated to the operation and maintenance of certain existing equipment. A good example of this is the Coast Guard’s budget request for acquisitions in FY14, which is 37 percent lower than current levels. To cut that spending, the Coast Guard took a hatchet to a range of programs, including the Fast Response Cutter program and the HC-144A aircraft program.

CBP’s biggest acquisition areas – Air and Marine Operations and Procurement, and Border Security, Fencing, Infrastructure and Technology – suffered cuts in the president’s budget request. However, it is noteworthy that CBP protects its Integrated Fixed Towers program, which may offer some encouragement to companies competing for that program. In addition, CBP proposes bolstering its staff, paying for new officers in part by charging new fees.

The TSA, one of the biggest beneficiaries of consistent funding growth since its establishment more than a decade ago, saw a cut of more than 8 percent in the FY14 request. The bulk of this comes from the aviation security account, with several technology and equipment programs seeing cuts or delays. With much of TSA’s screening equipment nearing the end of its life, this area may be one in which Congress seeks to reverse the administration’s budget reductions.



## Homeland Security

While it may be tempting for Congress to restore select funding levels, particularly in the operational components, it is unlikely that action will lead to an overall increase in the budget. It is more likely to force cuts in other areas of DHS. Watch for cuts to easy targets like the Science & Technology Directorate and the St. Elizabeth’s Campus effort, particularly as the House moves through its appropriations process.

Given the importance of securing computers and information in the government and the private sector, the National Protection and Programs Directorate – which oversees this area, both operationally and policy-wise – received a boost of more than 9 percent for cybersecurity efforts, despite a flat budget overall for the organization.

For vendors selling to DHS, the bottom line is this: The FY14 budget request represents a new level of austerity that does not produce many new business opportunities. If it is enacted into law, expect to see incumbents fight like mad to keep existing business, and expect steep competition (and fewer dollars) for new opportunities.

From a policy perspective, the budget request renews some fights DHS has picked – and lost – in the past, including an effort to consolidate a series of grant programs into a single “National Preparedness Grant Program.” Additionally, new TSA fees to help bolster the organization’s capital expenditure accounts have been proposed again for FY14. This concept, however, has been repeatedly rejected by Congress each time it has been offered, and there is no reason to believe this year will be any different.

It’s likely that the House will send 12 appropriations bills to the Senate. Once that happens, though, it’s anyone’s guess as to what the Senate will do. There does not seem to be a clear process in that chamber for moving legislation through regular order. Therefore, it is likely that continuing resolutions will set appropriations levels for FY14, as they have done for most of the government during the current fiscal year. ■

*Andrew Howell is a Partner at Monument Policy Group, a Washington D.C.-based government relations consulting firm.*

THANK YOU!

SIA GOVERNMENT

2013

SUMMIT

WASHINGTON, DC | JUNE 4-5

[siaonline.org/summit](http://siaonline.org/summit)



United Technologies

Climate | Controls | Security



tyco  
Integrated Security

SIEMENS



Honeywell



Panasonic



SECURITY SALES & INTEGRATION



# Immigration Bill Provides Billions for Border Security Enhancements

By: *Romina Boccia*

The contentious immigration bill (S. 744) put together by the Senate Gang of Eight includes a number of “border security” features to be paid for by exploiting a loophole in the Budget Control Act. By designating spending in the immigration bill as “emergency requirements,” the bill would enable lawmakers to spend billions outside existing budget enforcement procedures. So much for the spending caps and sequestration procedures agreed to in 2011.

Section 6 of the bill would establish a Comprehensive Immigration Reform Trust Fund and provide \$6.5 billion in funding from general revenues, which includes:

- \$1 billion for startup costs, including application processing.
- \$3 billion for the Comprehensive Southern Border Security Strategy over five years.
- \$1.5 billion for additional fencing in high-risk border sectors over five years.
- \$2 billion for the Department of Homeland Security (DHS) to pursue “persistent surveillance” and an effectiveness rate of 90 percent or higher over ten years.

Sens. Schumer, Graham, Durbin and Flake amended their original bill in May. One new provision is that the first \$7.5 billion collected by the new immigration trust fund from visa fees and penalties for false statements in applications be paid back to the Treasury Department for deficit reduction. This is an improvement over the spend-as-you-please approach taken in the first draft. Unfortunately, it adopts a spend-now-save-later approach, effectively replacing one budget gimmick with another. Funds for the activities identified below would be authorized only after Treasury was paid back:

- \$50 million per year to increase the number of border crossing prosecutions to 201 prosecutions per day, and
- \$50 million each year for Operation Stonegarden (90 percent to be allocated toward grants and reimbursements to Southwest border state law enforcement agencies).

Section 1106 of the bill would provide funding for equipment and technology as necessary. That would be in addition to any appropriated funds for U.S. Customs and Border Protection from 2014 through 2018, including for agent-portable surveillance systems; unarmed, unmanned aerial vehicles (to be deployed 24/7 along the southern border); unarmed additional fixed-wing aircraft and helicopters along the southern border; and new rotocraft and upgrades to the existing helicopter fleet.

Section 1107 of the bill would provide grants as necessary for individuals residing or working in the border region who lack

cellular service to purchase satellite telephone communications services able to dial 911 and equipped with GPS. Section 1107 would further provide funds as necessary for five years to purchase P25-compliant radios, which may include a multi-band option, for Southwest border federal, state and local law enforcement agents through a competitive procurement process. It also would provide funds to upgrade the Department of Justice’s communications network.

Authorizing such funding “as necessary” lacks accountability and transparency. Just how much or how little funding is necessary, and how will that be determined?

A recent article by Heritage Vice President for Foreign and Defense Policy Studies, James Carafano, illustrates why the spending in this bill does not meet any objective criteria of emergency requirements. Carafano explains that, according to DHS Secretary Janet Napolitano, America’s borders “have never been more secure,” and the White House has not asked for this additional border security funding in more than five years. The immigration bill, however, would spend billions on border security enhancements, largely as part of a political deal in exchange for amnesty. ■

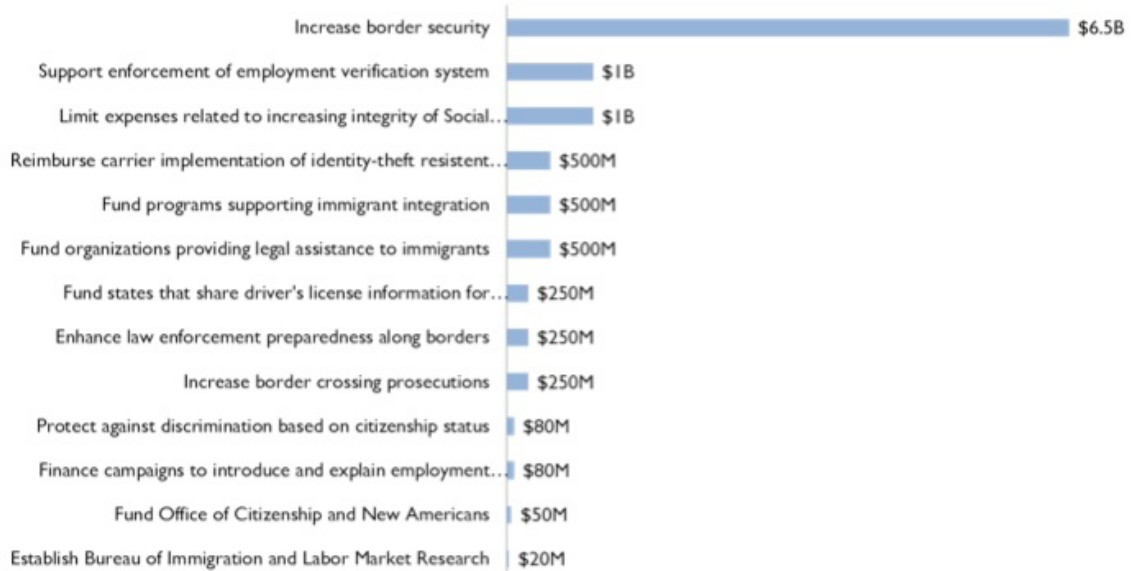
*Romina Boccia, an economist, is assistant director in the Heritage Foundation’s Roe Institute for Economic Policy Studies, where she analyzes federal spending and legislation. Romina can be reached at Romina.Boccia@heritage.org. Follow her on twitter @RominaBoccia.*



Figure 1

## Immigration Bill Allocates Most Funds to Border Security

Funding Allocations in the Border Security, Economic Opportunity, and Immigration Modernization Act (FY 2013-2023)

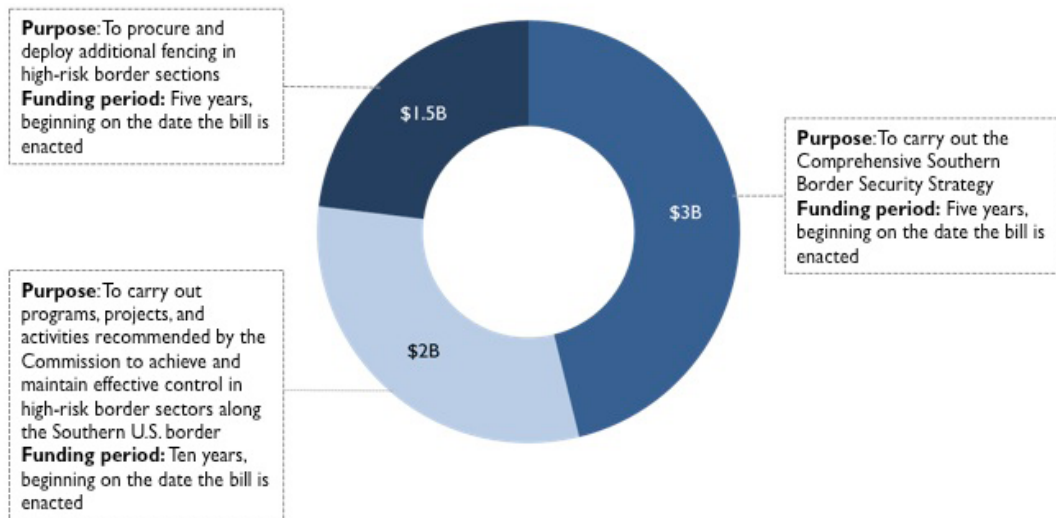


Source: Border Security, Economic Opportunity, and Immigration Modernization Act.  
Image courtesy of National Journal <http://www.nationaljournal.com/membership/document/4185#> April 18, 2013

Figure 2

## Immigration Bill Allocates \$6.5 Billion for Border Security Initiatives

Breakdown of Funding for Increased Border Security in Border Security, Economic Opportunity, and Immigration Modernization Act



Source: Border Security, Economic Opportunity, and Immigration Modernization Act.  
Image Courtesy of National Journal <http://www.nationaljournal.com/membership/document/4188>, April 18, 2013

**NOTE:**

For more information about this publication, contact Marcus Dunn, SIA director of government relations, at 301.804.4712 or [mdunn@securityindustry.org](mailto:mdunn@securityindustry.org), or Elizabeth Hunger, SIA manager of government relations, at 301.804.4714 or [ehunger@securityindustry.org](mailto:ehunger@securityindustry.org)

# Gearing up for TWIC Readers – Maybe Not

By: *Walter Hamilton*

The U.S. Coast Guard has finally published its Notice of Proposed Rulemaking (NPRM) to establish the regulatory requirements for using access control readers in conjunction with the Transportation Worker Identification Credential (TWIC) smart card. As required by the Maritime Transportation Security Act of 2002, the Transportation Security Administration (TSA) has issued more than 2 million TWIC cards to civilian maritime workers who require unescorted access to secure areas of regulated maritime facilities and vessels. The proposed TWIC reader regulations appeared in the Federal Register on March 22 and public comments were accepted through May 21.

For those who believe in using technology to enhance physical security, this proposed regulation is a major disappointment. The big news is that the Coast Guard is waiving the requirement to implement TWIC readers for all but the highest risk facilities and vessels as determined by a complex risk assessment and cost analysis process. In fact, the Coast Guard estimates that only 5 percent of TWIC holders will be required to use access control readers with their TWIC cards when accessing secure areas. Under this proposal, 532 of 3,270 regulated facilities and only 38 of nearly 14,000 vessels would be required to implement TWIC readers at entry points.

For the other 95 percent of entry transactions, the Coast Guard requires only visual inspection of TWIC cards by security personnel. The rationale for using the TWIC card as a “flash pass” by the majority of maritime operators appears to be that the Coast Guard does not believe that these operators face security risks that justify the costs and other burdens that would result from a broader requirement for readers. What is most alarming is that most petro-chemical and large container terminal facilities are ranked in the lower risk category and, thus, are not required to use readers for worker access. The Coast Guard’s risk assessment does not appear to consider the negative impact to the nation’s economy that would result from the disruption of any of these critical infrastructure facilities.

TSA designed the TWIC card as a tamper-resistant, biometrically-enabled, dual-interface smart card with sophisticated security features that allow for electronic validation, expiration checking, revocation checking, and biometric verification of the card holder. But instead of taking full advantage of this advanced security technology, the Coast Guard plans to require only visual inspection of the TWIC card for 95 percent of entry transactions. Apparently, the Coast Guard believes that visual inspection is an adequate authentication mechanism for physical access. Security industry professionals do not share that view.



First, visual inspection of TWIC cards is subject to human error and is not an effective method of detecting counterfeit cards. Reliance on visual inspection will encourage a black market in high-quality fake TWIC cards that can be easily obtained through the Internet.

Second, biometric verification is the only way to confirm that the cardholder is the same person to whom the card was originally issued. Visual comparison of a photo to the person is simply not reliable or consistent.

Third, it is impossible for security personnel to visually detect that a TWIC card has been revoked by the government. If TSA receives a report that a TWIC card has been lost or stolen, or that a TWIC holder is now identified as a security threat, the agency will immediately add the TWIC card identifier number to its published TWIC Cancelled Card List (CCL). But only a TWIC reader can read the unique card identifier number and compare it with TSA’s CCL. The identifier number is not printed on the card.

Finally, the National Institute of Standards and Technology (NIST) recently established that visual inspection provides “little or no assurance of identity” when used for access to government facilities. In fact, use of visual inspection as an authentication mechanism is discouraged in the most recent government standards for personal identity verification of government workers and contractors.

Congress clearly did not contemplate that just 5 percent of maritime workers would use electronic access control readers when it enacted the law that required issuance of a biometric transportation worker card. Security industry organizations have been encouraged to submit comments to the Coast Guard stating that visual inspection provides little or no assurance of the identity of the TWIC holder and is not sufficient to protect our nation’s critical maritime infrastructure from a terrorist security incident. ■

*Walter Hamilton is a senior consultant with Identification Technology Partners, Inc., and is vice chairman of the International Biometrics & Identification Association (IBIA). He has been an active participant in the TWIC program since its inception in 2005. Walter can be reached at [whamilton@idtp.com](mailto:whamilton@idtp.com).*



# Benghazi Attacks Spur Calls for Increased Embassy Security

By: Rachel Hoffman and Elizabeth Hunger

The Sept. 11, 2013, terrorist attacks on the U.S consulate in Benghazi, Libya, claimed the lives of Ambassador Christopher Stevens, Sean Smith, Tyrone Woods and Glen Doherty. In the months since the attack, the Obama administration has been harshly criticized for its approach to embassy security. This tragic event forced lawmakers to rethink and revamp the protections we provide Americans living in and working at diplomatic posts abroad.

While the attacks in Benghazi served as a harsh wake-up call for many lawmakers and administration officials, embassy security is not a new challenge for the State Department. Incidents such as the attack on the U.S. Embassy in Ankara, Turkey, in 1958, the seizure of the U.S. embassy in Iran in 1979 and the 1998 bombings at U.S. embassies in Dar es Salaam, Tanzania, and Nairobi, Kenya, serve as grim reminders that the Americans in the United States' 283 diplomatic facilities worldwide face serious security challenges.

The year after the 1998 attacks, Congress passed the Secure Embassy Construction and Counterterrorism Act (SECCA). This legislation authorized appropriations to the Department of State for the construction and security of U.S. embassy facilities. The State Department has two programs whose missions are dedicated to embassy security: the Bureau of Overseas Building Operations (OBO), which focuses on physical security, and the Bureau of Diplomatic Security (DS) which deals with security programs. As of February 2013, approximately \$10 billion has been appropriated, 97 new diplomatic facilities have been completed and an additional 37 are under design or construction.

However, the incident in Benghazi leads to the question; are we doing enough?

In mid-February, Patrick Kennedy, the undersecretary of state for management, testified before the House Appropriations' Sub-

committee on State, Foreign Operations, and Related Programs. Kennedy said that, despite the achievements that have been reached under SECCA, "there remain approximately 158 posts that have facilities that may not fully meet current security standards." He went on to note that, "many of these facilities were built or acquired prior to the establishment of the current security standards, and others are subject to authorized waivers and/or exceptions."

In his budget request for 2014, President Obama responded to a recommendation by the independent Benghazi Accountability Review Board by including \$2.2 billion in funding for embassy security construction at hundreds of diplomatic posts across the globe. Included in this amount is \$95 million for compound security, an increase of \$10 million from 2013. Also included is \$525 million for Capital Security Cost Sharing, a program designed to spread the costs of embassy construction across multiple government departments based on that department's level of involvement and presence at a particular embassy.

The men and women of the U.S. diplomatic corps know and accept that their responsibilities may take them to countries and regions plagued by violence, conflict and insecurity. However, they deserve to know that the facilities in which they work and live meet the highest possible standards for physical security, including access control systems, surveillance equipment and strong perimeters. It is the duty of the federal government and the security industry to provide foreign diplomatic missions with the security technology and resources required for them to continue effectively promoting American values and interests overseas. ■

Rachel Hoffman is an intern with the Security Industry Association. She is a recent graduate of Georgetown University and a Fulbright Scholar. Elizabeth Hunger is the manager of government relations for the Security Industry Association. She can be reached at [ehunger@securityindustry.org](mailto:ehunger@securityindustry.org).

<b>Budget Comparison: Foreign Embassy Security, Construction and Maintenance</b>	<b>FY 2013 BUDGET</b>	<b>FY 2014 BUDGET</b>
	<b>(UNDER CONTINUING RESOLUTION)</b>	<b>(PROPOSED BY PRESIDENT)</b>
Total new obligations for embassy construction, security and maintenance	<b>\$3.30 billion</b>	<b>\$3.15 billion</b>
Capital Security Construction	<b>\$1.1 billion</b>	<b>\$950 million</b>
Capital Security Cost Sharing	<b>\$450 million</b>	<b>\$525 million</b>
Operations	<b>\$85 million</b>	<b>\$95 million</b>
Repair and Construction	<b>\$850 million</b>	<b>\$800 million</b>
Overseas Contingency Operations (OCO)	<b>\$550 million</b>	<b>\$200 million</b>
Total direct program funding not including Overseas Contingency Operations	<b>\$33 million</b>	<b>\$163 million</b>
Total direct program funding including Overseas Contingency Operations (OCO)	<b>\$2.47 billion</b>	<b>\$ 2.2 billion*</b>
	<b>\$2.50 billion</b>	<b>\$2.363 billion</b>

\* IN ADDITION TO THE \$2.2 BILLION FOR SECURITY CONSTRUCTION FUNDING, \$163 MILLION HAVE BEEN ALLOCATED FOR OVERSEAS CONTINGENCY OPERATIONS (OCO). IN THE FY 2014 BUDGET, THE PRESIDENT CHOSE TO SEPARATE THIS FUNDING FROM THE REST OF THE ALLOCATIONS FOR EMBASSIES.

SOURCE: "EMBASSY SECURITY, CONSTRUCTION, AND MAINTENANCE." DEPARTMENT OF STATE AND OTHER INTERNATIONAL PROGRAMS - BUDGET YEAR FOR 2014. PAGE 802. [HTTP://WWW.WHITEHOUSE.GOV/SITES/DEFAULT/FILES/OMB/BUDGET/FY2014/ASSETS/STA.PDF](http://www.whitehouse.gov/sites/default/files/omb/budget/fy2014/assets/sta.pdf).

**ALL NEW  
FOR 2013!**

**ANNUAL BARNES/SSN STUDY**  
**Wholesale monitoring  
results revealed** See page 21

**IT'S SHOWTIME: ISC WEST 2013**  
**Preview show products  
before you go** See page 46



**SECURITY SYSTEMS NEWS**  
THE NEWSPAPER OF RECORD FOR THE SECURITY SYSTEM INTEGRATOR & INSTALLER

VOLUME 16, NUMBER 4  
APRIL 2013 • \$7.00  
COMMERCIAL SYSTEMS

**Unlimited Technology gets  
a new chairman and CEO**

**SAFE  
Security embarks  
on new  
chapter**

A SUPPLEMENT TO  
**SECURITY SYSTEMS NEWS**

**SIA**  
**FISCAL YEAR INFORMER**

- Budget Battles**  
The private sector weighs in on sequestration **3**
- Obama's Technology Agenda**  
A look at the technology agenda under the new Obama Administration **6**
- Top 10 Grant Mistakes**  
Common mistakes to avoid when applying for grants **10**

Q1: 2013

Houston and Valhalla, N.Y., UTI did about \$20 million in sales in 2012 and has 65 employees. It is a PSA Security owner.

Rockwell is no stranger to the security industry. He was the majority shareholder and served as a chairman of Henry Brothers Electronics before it was sold to Kratos Defense and Security Systems in 2010.

Rockwell is currently owner and chairman of three security companies: Main Security Surveillance in Augusta, Maine,

since 2005; New York Merchants Protective Co. in Mineola, N.Y., since late in 2011; and 123 Lock & Key in Bristol, N.H., which has been part of Main Security Surveillance since 2011.

Asked if there are any synergies among the four security companies he's involved in, Rockwell said yes.

"There are a lot of synergy affiliations and we're looking forward to a whole new kind of help desk, intimacy with the customer [and] remote diagnostic capability, all wrapped up in a warm, fuzzy human wrapper," Rockwell told Security Systems News.

**UNLIMITED** see page 26



R. Rockwell

It is growing its dealer program, expanding into DIY, bought 35,000 accounts from Pinnacle and has a new equity partner

By Tess MacLewicz  
SAN RAMON, Calif.—SAFE Security is offering a \$10,000 bonus to dealers who sign up by the last day of ISC West this year, the company announced in March.

The announcement is the latest development from one of the nation's largest full-service security companies. It is based here and now does business in 46 states.



Paul Sargentini

In the past few months, SAFE also got a new private equity owner, bought 35,000 accounts from Pinnacle Security—which allowed it to expand into Alaska and New Mexico—and launched a new DIY division, with which it hopes to tap into the rental market.

"It's a very exciting new chapter for SAFE," President and CEO Paul Sargentini told Security Systems News. He said the recent developments are all part of a plan to

**SAFE** see page 41

**Vivint gets into R&D**  
Security and home automation provider opens Innovation Center with 50 engineers, designers

by Martha Entwistle  
SALT LAKE CITY, Utah—With the goal of being "vertically integrated" and in control of all components of its offerings, security and home automation provider Vivint announced that it has opened the Vivint Innovation Center here.

"We want to make sure we continue to innovate around the products and services that we provide to customers," Alex Dunn, Vivint president, told Security Systems News.

Vivint's hardware had been provided by 2GIG Technologies. On Feb. 14, Nortek/Linear announced it had acquired 2GIG and said the deal included a five-year service agreement with Vivint.

Dunn explained that Vivint will



Vivint will design and test new technologies in the company's recently opened Innovation Center.

develop its own proprietary panel which Linear will manufacture for Vivint. The announcement was made on Feb. 15, but the 30,000-square-foot center is already up and running with 50 hardware, software and radio engineers, industrial designers and user-experience professionals.

Dunn said that some of the center's engineers previously

**VIVINT** see page 44

A SUPPLEMENT TO  
**SECURITY SYSTEMS NEWS**

**SIA**  
**FISCAL YEAR INFORMER**

FOUND WITH THESE UPCOMING ISSUES OF

**SECURITY SYSTEMS NEWS**  
THE NEWSPAPER OF RECORD FOR THE SECURITY SYSTEM INTEGRATOR & INSTALLER

