Campaign

A Candidates and Voters Guide to Security Reform
Dear Candidates and Voters,

When it comes to keeping the United States strong and safe, national security is the first responsibility of government. However, given today’s threats and challenges—to our stature and security in global affairs, to our homeland security, to our energy and cyber security—government and our military is not enough. Every American, candidate and voter alike, has a unique opportunity and a responsibility to contribute in common cause.

The private sector has a unique opportunity to contribute. The same entrepreneurial spirit that inspires American business can help transform the business of national security—how the United States government and our armed forces meet and defeat the security threats to our country.

What can we learn from the successes and failures of individuals and businesses that will lead to greater achievement in meeting evolving challenges to our government and national security enterprise? The following pages offer assessments and solutions to specific concerns ranging from sustaining the nation’s economic security to managing for efficiency, attracting talented individuals to serve in government, and strengthening our domestic security establishment.

Business Executives for National Security (BENS) is proud to offer this guidebook for innovative new approaches to these problems. For over thirty years, BENS has worked with government officials, the military, and with leaders from both political parties using the insights, expertise and best practices of the private sector to help build a more secure America—embraced by Democrats, Republicans, and Independents alike.

If you need additional information on any of the topics in this guide, please visit our website at www.BENS.org or contact us by email at policy@bens.org.

General Norton Schwartz, USAF (ret.)
President & CEO
1. Economic Security
2. Domestic Security
3. Efficiencies at the Department of Defense
4. Cyber Security
5. Talent Management at the Department of Defense
6. Internet Governance
7. Reducing Government Infrastructure
8. Making Senior Government Service More Attractive
The Challenge:

America’s national security is founded upon our economic security; however, our current spending trajectory is unsustainable and the interest on our national debt is projected to become the fastest growing part of the budget, which threatens the resources available to equip our troops and defend our interests.

- Neither the Congress nor the current Administration are focused on the long-term fiscal issue; with the former dividing along predictable party lines on taxes, entitlements, and spending, and the latter focused on issues it considers more manageable.

- The current two-year budget agreement restores about 90% of the sequester imposed by the Budget Control Act of 2011. It expires in 2017 re-imposing cuts across defense and entitlement programs without regard to fairness, appropriateness, or the risk of unintentional outcomes.

- Prolonged annual budget debates prevent agencies from effective budget planning or budget execution. Government shutdowns and continuing resolutions further exacerbate economic difficulties without providing needed fiscal reforms.
A New Approach:

- Civic, and business leaders—the latter of which are notably absent from the debate—need to demand that their political leaders address the fiscal crisis in a responsible fashion.

- The U.S. needs to objectively examine federal spending and decide on national priorities in light of constrained fiscal resources.

- Congress needs to enact, and the President needs to implement, laws that have the same amount of deficit reduction as current law, but with a more sensible mix of revenue increases and spending cuts.

- The national security budget must adjust to steady or declining financial resources, and adjust in a fashion to adequately match strategy.

Frequently Asked Questions:

What is the primary factor contributing to our national debt?

Healthcare is the major cost driver of our fiscal crisis. Medicare and Medicaid today account for 23 percent of the federal budget. In 2013, national health expenditures represented 17.4 percent of GDP. Without reform, by 2024 healthcare spending will represent 19.6 percent of GDP, reflecting a 12.6 percent increase.

What will happen to our spending for national defense if nothing is done?

The practical effect is that core defense spending will fall as a percentage of GDP from nearly 4 percent today to 3 percent in 2019, and from 20 percent of total federal spending today to 11 percent in 2040. The resources for national security will face no real opportunity for growth and, quite possibly, will see a decline unless other areas of discretionary spending and debt service can be controlled.
The Challenge:

The terrorist threat to the U.S. has proven to be durable and dynamic. Despite numerous reforms since 9/11, the U.S. still lacks an enterprise-wide concept for its domestic security efforts, a unified domestic threat assessment, and the capacity for synchronized actions at all levels of government.

- Since 9/11 there has been a proliferation of intelligence and counterterrorism-related entities, and yet there is still no clear federal leader managing U.S. domestic security efforts overall, nor is there a unified domestic threat assessment accounting for federal, state, and local priorities.

- Collaboration between state and local officers and their federal counterparts—particularly at state and local fusion centers—remains uneven and ad hoc.

- Career incentives and professional development opportunities for domestic intelligence analysts at all levels of government are underdeveloped, and training opportunities and resources for state and local law enforcement officers remain limited.
A New Approach:

- Empower a senior federal official to provide strategic management of federal domestic security efforts; lead an annual interagency domestic threat assessment; and ensure appropriate civil liberty protections.

- Co-locate field-level entities wherever practical to enhance analytic capacity, provide a consolidated hub to receive and disseminate intelligence products, and reduce the duplicative costs associated with multiple operating locations.

- Enhance the investigatory awareness of intelligence and law enforcement officers by creating investigative review groups at the field-level composed of FBI and state and local officials to facilitate the real-time exchange of information of ongoing and closing investigations.

- Encourage the service, development, and retention of high-quality domestic analysts by developing standardized training; increasing leadership opportunities and joint duty assignments; and providing state and local officers with greater access to these training and professional development resources.

**Frequently Asked Question:**

*How can we properly protect our civil liberties and expectation to privacy while also confronting these threats?*

In a free and open nation such as ours there will always be a need to seek a balance between security and civil liberties. Strengthened domestic security efforts must be conducted within an explicit legal framework, with respect to due process, and in pursuit of a transparent judicial end-game. Enhanced training, clear federal management, and effective Congressional oversight can both ensure our public safety and reinforce our civil protections.
The Challenge:

Over the past decade, military support functions like logistics and transportation have grown 7% annually, consuming 40% of total defense spending. Inefficient defense business practices are compounded by the failure to pass budgets within regular order, making it difficult for the Defense Department to plan and perpetuating a dynamic in which resources drive strategy.

- From 2001-2014, the active duty military shrank by approximately 3%. During this same time period, the civilian workforce grew by about 10% to 756,000. In addition, DoD’s civilian contractor workforce has grown to an estimated 700,000.

- Overhead in headquarters has ballooned. The joint staff now numbers nearly 4,000 members; the nine globally-disbursed combatant command staffs number over 38,000; and, the staff in the Office of the Secretary of Defense numbers more than 5,000.

- The Defense Department recently added 27,000 new acquisition positions, but unless it streamlines the costly, inefficient and slow process of acquiring goods and services, the added workers will not contribute materially to positive, business-driven outcomes.
A New Approach:

• The Defense Department requires an enterprise-wide business plan that connects its strategy to its budget, linking the military force America needs and associated missions with necessary resources. The Quadrennial Defense Review no longer serves this purpose.

• The headquarters staffs need to be economized and redundancies between the military service’s civilian and military staffs need to be resolved. Current Congressional plans to review the 1986 Goldwater-Nichols legislation needs to include consolidation of headquarters establishments.

• To achieve improvements in performance, cost, and delivery timeframes for new weapons, the acquisition process should involve warfighters who understand combat, engineers who understand technology, and financial experts who can accurately measure the costs and the ability to trade among these factors to achieve fielded systems.

• The Defense Department should transparently and comprehensively justify bringing contract work in house, while carefully weighing the risk that doing so will diminish the contract opportunities for private industries on which the military relies.

Frequently Asked Question:

Why can’t the Defense Department be run like a business?

No one will make a convincing case that the deployable side of the Defense Department—the warfighters on the battlefield—should be run as a business. But the Operations and Support side, which consumes almost 70 percent of the military’s annual budget, is largely geographically-fixed and structured like a business with logistics, transportation, finance and human resources. Those elements of the Pentagon can and should adopt best business practices.
The Challenge:

Information and communications technology is increasingly essential for most elements of daily life, but is vulnerable to disruption, illicit activity, and abuse. Weak security practices exacerbate cyber vulnerabilities, and fragmented authorities, decentralized ownership of infrastructure, and legal or privacy considerations affect defense and response.

- Ambiguities persist on whether, how, and under what circumstances industry and government can cooperate on cybersecurity matters.
- Public-private partnership on cyber issues is frequently discussed but remains underdeveloped and insufficiently employed.
- Government agencies hold sensitive information, but rely on legacy infrastructure, often lack the skilled workforce necessary to increase security, and still lack sufficient means to identify, penalize, or deter malicious cyber activities.
- In industry and government alike, decision makers face enormous uncertainty in estimating their exposure to cyber-related risk, and often under-resource security measures.
- Long delays in discovering breaches leave consumers exposed to significant privacy and security threats, while weak organizational response plans, jurisdictional issues, and inconsistent reporting requirements complicate...
A New Approach:

- Industry and government should increase their cooperation where possible by deepening institutional relationships, understanding each other’s constraints, and where necessary clarifying relevant laws and policies.

- Government agencies must vigorously and continuously monitor their cybersecurity performance, and foster an environment of greater accountability for failures. Independent assessments should guide corrective efforts.

- Both inside and outside of government, organizations’ senior leadership should assume more responsibility for cybersecurity, from setting security performance standards to contingency planning, and premise this deeper engagement on an intimate understanding of risks specific to their organization’s most valuable assets.

Frequently Asked Question:

What federal agency is responsible for partnering with the private sector on cybersecurity issues?

Several Executive Branch organizations have cybersecurity related investigative, support, and partnership mandates. The Federal Bureau of Investigation offers key investigation and response capabilities, while the Department of Homeland Security is attempting to enhance information sharing mechanisms, education, alerting, and other means to protect assets. One constant is that, in the event of a breach, preexisting relationships between private sector organizations and government agencies are enormously helpful.
The Challenge:

Increases to personnel costs threaten to hamper DoD’s ability to buy weapons, train, and conduct operations. Burgeoning recruitment challenges threaten to erode the military services’ competitive advantage. Today, approximately 50 cents of every DoD dollar is spent on personnel costs, and there is keen competition with the private sector for top employees.

- The All-Volunteer Force has been a resounding success since its formulation in 1971. However, compensation and benefit policies are now antiquated and reflect neither private sector practices nor the specialized needs of the military services.

- The purpose of efforts to reform personnel practices is misplaced. DoD benefits packages and talent management practices are not about maintaining troop numbers, they are intended to ensure the most capable workforce is available and properly equipped to win wars.

- The human resource enterprise within the Department suffers from a status quo bias and has proven resistant to change. Bureaucratic inertia has contributed to the maintenance of a 40-year old personnel system.
A New Approach:

- The Fiscal Year 2016 National Defense Authorization Act included a new hybrid retirement system for the uniformed military, combining both defined benefit and defined contribution attributes. This modernization effort should be fully supported.

- The military services must continually examine its recruitment processes to stay competitive. Evolved and improved talent management practices within the uniformed services are prudent and, ultimately, war-winning actions.

- The one-size-fits-all, tenure based system of the present should be replaced by a system characterized by customizable paths of service in which individual talents can be more accurately assessed, developed, and rewarded.

Frequently Asked Questions:

**Why is it necessary to revisit military compensation and benefits if the All-Volunteer Force is such a success?**

Compensation and benefit programs have been allowed to grow with insufficient reference to the actual human capital needs of the military services.

**If the services keep hitting their recruiting and retention targets, why is reform of the personnel system required?**

Our servicemembers of the past and present have exceeded expectations in all that we have asked of them. In order to make the same statement in 10-20 years, we must continue to stress the quality of our force without being distracted by simplistic, industrial age metrics emphasizing quantity.
The Challenge:

How the Internet is governed is critically important to our economy and national security, yet few appreciate its overall significance. Emerging changes in Internet governance underscore the importance of maintaining a coherent, sustainable approach to the issue. Failure could lead to structural changes that risk fragmenting the Internet.

- An open and diverse but relatively small group of stakeholders make consensus-based decisions with enormous implications for the future of the Internet.
- Real and perceived barriers to participation and active contribution—such as wide geographic dispersal of relevant coordinating meetings and concerns about technical qualifications, respectively—compound a general lack of understanding about the issue.
- In some instances, stakeholders have viewed security as a tactical matter disassociated from broader discussions about governance and accountability of coordinating bodies.
- Abroad, some governments have discounted multistakeholder-based approaches and allowed narrow, strictly-governmental interests to define national policy positions.
A New Approach:

- Businesses, civil society stakeholders, and others must actively monitor and participate in Internet governance discussions, most notably within Internet Corporation for Assigned Names and Numbers (ICANN) processes.

- U.S. policymakers at all levels must recognize the importance of Internet governance, familiarize themselves with relevant policy issues, model the international implications of different courses of action, and provide reasonable oversight where appropriate.

- Multistakeholder community members must elevate security to a core issue in discussions about the future of Internet governance and enhancements in coordinating bodies’ accountability.

- U.S. private sector leaders can help impress upon counterparts abroad the importance of an inclusive model for Internet governance, wherein governments alone cannot dictate decisions and outcomes.

Frequently Asked Question:

*Can someone without deep technical knowledge meaningfully contribute in Internet governance discussions?*

Yes. Internet governance discussions can range from deeply technical to completely nontechnical in nature. Recent and ongoing discussions about enhancing ICANN accountability, for example, involve a host of legal, policy, institutional design, and process issues that do not require a technical background to understand.
The Challenge:

Although the first four rounds of the Military Base Closure and Realignment (BRAC) process are producing an annual recurring savings of approximately $8 billion, the Pentagon continues to maintain more than 20% excess domestic facility capacity. Similarly, the Department of Homeland Security has been criticized for inadequate real property management.

- The President’s defense budget last year included an annual request for new BRAC authority, but has not included dollar estimates because the Pentagon knows it is a politically fraught decision.

- Congress reinforced the Department’s half-hearted request by inserting language into its recent Defense Authorization legislation to prevent DoD from spending money for even planning for a new round of BRAC.

- Inattention to cost growth in implementing the 2005 BRAC program—an estimated cost of $21 billion to implement the program had grown to $35 billion by September 30, 2011—cast doubt on base closure as a way to save money.

- The Department of Homeland Security established a joint requirements council to look for efficiencies and ways to reduce redundancy. It is not clear that the process is focused on or has resolved existing real property management inadequacies.
A New Approach:

- The Defense Department’s impending resource constraints warrant reauthorization of the base closure legislation with another round to occur not later than 2017.

- BRAC is one of the few tools the President and his Secretary of Defense have to shape and transform defense support infrastructure. The focus must be on reducing, not repurposing, excess infrastructure.

- Past BRAC rounds have occurred without benefit of a strategic perspective. The Department needs to create a base structure planning document that describes to Congress and the taxpayer the types of facilities needed to support our military objectives over the next decade.

- The Government Accountability Office maintains a high risk watch on DHS real property. Congress needs to step up its oversight to ensure that proper follow-through on infrastructure consolidation and reduction continues throughout the Department.

Frequently Asked Question:

*Why doesn’t the Department of Defense just cease unneeded operations, lease closed facilities and reduce workforce through attrition rather than go through the formal BRAC process?*

History shows that any non-BRAC attempt to close or realign a base will encounter political opposition. The BRAC process is thus indispensable to the Pentagon’s efforts to shed unnecessary and costly infrastructure. Besides, BRAC gives the Department certain authorities to transfer closed bases directly to local communities for reuse rather than going through more lengthy government property disposal processes.
The Challenge:

Selecting qualified candidates to fill civil positions—especially the top national security offices—in the Executive Branch is a significant responsibility for the President. Deterrents to public service, such as financial disclosure rules, confidentiality, and post-employment restrictions have become a hindrance to attracting the best-qualified individuals.

- During a Presidential election cycle, the naming of a transition coordinator or a transition team early in a political campaign is too often deemed to be presumptuous and, therefore, not a priority.

- The appointments system lacks openness and precision. Even in this digital age records to keep track of presidential appointees prove to be less than comprehensive. Information on positions and vacancies are dependent on accurate agency reporting, which is often insufficient.

- The confidentiality of background investigation results is tenuous. A full-field FBI investigation acquires uncorroborated information comingled in the report. Whether laudatory or damaging “leaked information” proves a deterrent to candidates.

- The financial disclosure requirements are extensive. Considerable time and effort is required to collect investment income data as well as to meet the minimum disclosure thresholds, which have not been adjusted since set by law in 1978.
A New Approach:

- Build the pre-election Presidential transition teams to be large enough to evaluate and rank candidates for the top 50 national security positions at the beginning of an administration.
- Complete the process of eliminating duplication and removing extraneous information in the required application forms and financial disclosure documents.
- Convert more presidential appointees to career status Senior Executive Service and “Schedule C” appointments; and, expand the concept of “privileged nominations” in which candidates are placed directly on the Senate’s Executive Calendar instead of being referred to committee.
- Review conflict of interest provisions with an aim to increasing the range of remedies permitted short of divestiture of financial instruments. Refine post-government employment restrictions.

Frequently Asked Questions:

Why is it that the presidential appointment process from candidate selection to Senate confirmation is taking longer and longer to complete?

Part of the delay is the lack of processing capacity on the part of the president’s transition teams; however, a growing cause is the complexity and length of the vetting process before a nomination is even made. The nomination process actually accounts for more delay in moving nominees into presidential appointments than does awaiting Senate confirmation.