INTERNET
SECURITY
ALLIANCE
www.isalliance.org

# EXECUTIVE SUMMARY
# ASSESSING PRESIDENT OBAMA'S EXECUTIVE ORDER ON CYBER SECURITY

Upon realizing that comprehensive cyber security legislation to address the nation's growing cyber security problem was unlikely to pass the Congress, President Obama issued an Executive Order on the subject in February 2013.

The Order marked a watershed moment in cyber security policy. For the first time, the head of a major power offered a unique approach to cyber security that departed from the traditional model wherein government would regulate industry behavior through mandates and prescriptions. Instead, the President outlined a partnership approach that could keep pace with the rapidly evolving threat while engaging industry, which owns and operates the vast majority of the critical infrastructure, to continually upgrade its cyber security on an economically sustainable basis.

The Order tracked many of the policy proposals that the Internet Security Alliance (ISA) had made in its 2008 report "The Cyber Security Social Contract," a publication that was also the first and most cited source in the President's 2009 "Cyberspace Policy Review." However, the Executive Order went beyond broad policy statements and identified specific actions that the Executive Branch agencies would take to implement the principles outlined in the earlier policy papers.

In particular, the Executive Order called for NIST to develop a "Cybersecurity Framework" of standards based on input from the private sector. This Framework would then be available to critical infrastructure owners and operators for voluntary adoption. Several Executive Departments were also charged with developing incentives to promote the Framework's adoption in lieu of regulatory mandates.

Now, roughly a year from the issuance of the Executive Order, it is appropriate to assess the progress that has been made under that Order and to assess whether the country's security will likely be enhanced as a result of its issuance. This paper offers five fundamental criteria that policy makers may use to analyze the progress made under the Order and suggests actions that Congress and Administration officials may undertake to fulfill the promise of the Executive Order. The five key questions this paper examines are:

1. **Does the Framework meet the "Cost-Effectiveness" criteria as required by the President's Executive Order?**
2. **Are we clear about what we are trying to do?**
3. **Has enough work been done on the incentives called for in the Executive Order?**
4. **Are we measuring our efforts appropriately and adequately?**
5. **Has the work under the Executive Order addressed the most serious of our cyber threats?**

### 1. Does the Framework meet the "Cost-Effectiveness" criteria as required by the President's Executive Order?

One of the key pillars of the President's Executive Order was the requirement for the National Institute of Standards and Technology (NIST) in conjunction with the private sector to develop a "Cybersecurity Framework" to enhance the security and resilience of the nation's critical infrastructure.

This Cybersecurity Framework was to include a collection of standards and practices culled from those that are already available, including from international standards where possible, to reduce the risk of harm to those assets that could impact national security. The Order also required the Framework to meet certain criteria. Specifically, the President's Order stated that:

> "The Cybersecurity Framework shall provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach…" Section 7(b).

While NIST has received widespread praise for the openness of the process it used to construct the Framework, it has not (at least to date) met the criteria specified by the President that is detailed above. Indeed, some critics have claimed that the Framework fails to meet nearly all of the criteria for adequacy identified in the President's Order.[i] Our focus here, however, is on the crucial area of cost-effectiveness.

The Executive Order was designed to create a voluntary program wherein owners and operators of critical infrastructure (as well as other private sector entities, potentially) would choose to adopt standards and practices identified in the Framework, which presumably they have not previously accessed, in order to protect their critical assets. According to the drafters of the Framework, this would be accomplished by encouraging these owners and operators to utilize a risk management approach to cyber security.

However, private sector operators (as well as government entities) routinely make security risk management decisions by including cost in their calculations. Indeed, independent research has consistently demonstrated that cost is the single biggest factor in critical infrastructure cyber security decisions.[ii], [iii], [iv] No private sector entity can be expected to make uneconomic (i.e., non cost-effective) security investments on a sustained basis.

As a result, the cost-effectiveness requirement in the President's Executive Order not only makes imminent sense, it is fundamental to the long-term success of voluntary adoption of the Framework.

If the Framework was demonstrated to be cost-effective, as required by the Order, then its voluntary adoption could be expected on the part of most, if not all, reasonable owners and operators.

The NIST Framework as currently constructed does not contain any analysis or data on the cost-effectiveness of potential implementation, either in whole or in part. Moreover, despite five nation-wide workshops sponsored by NIST, each with multiple breakout sessions (and despite private sector representatives bringing the issue up constantly), there was not a single session at any workshop devoted to a serious analysis of this topic.[v]

Without any information on the cost-effectiveness of the Framework, we are left with virtually no guidance for owners and operators on how to assess the utility of the Framework based on the most important two criteria that they and their shareholders must consider, namely:

- Will the adoption of the framework actually significantly improve our security?

- Will adoption of the Framework actually improve security at a reasonably viable cost so that the business can sustain its continued operation, profitability and competitiveness?

Explanations given by NIST are that it does not have the required economic expertise, and as cost-effectiveness varies between entities, only the entity implementing the Framework can properly assess its cost-effectiveness.

However, since cost-effectiveness is a criteria industry routinely needs to assess in making decisions, even absent Presidential mandates, there is plentiful expertise in the private sector (and likely within the government) that could provide assistance in addressing the issue.

Moreover, within the context of at least some critical infrastructures, variance of cost structures is not only largely consistent, but, in many cases, already used to assess other infrastructure requirements such as capacity and reliability. Certainly, a sampling of organizations within a defined set of critical infrastructure could yield useful data on this issue. Indeed, several private sector (as well as public sector) commentators to the NIST process have offered a pathway to address this issue as will be discussed in greater detail under question four.

Regardless of the reasons, the fact remains that the NIST Framework, arguably the foundational deliverable of the President's Order, fails to meet (or even seriously consider) the most important criteria specified in the Order: cost-effectiveness.

## 2. Are we clear about what we are trying to do?

To know if we are succeeding, we need to know what counts as success. Is it simply increasing awareness about managing cyber risk? Is it the percentage of entities that adopt, or use, the framework? Is it a significant reduction in successful attacks, or mitigation of the impacts of attacks? It is important to be clear as to what our specific goals are and determine some method to assess our progress in achieving these goals.

Lack of clarity on what counts as success can be dangerous by leading to a false sense of security. For example, policy makers need to understand that using the Framework is not the same thing as assuring critical infrastructure security—much more is needed. Such a misunderstanding could lead to misguided public policies. Similarly, senior executives need to be clear that funding IT budgets up to a level simply adequate to “adopt” or “use” the Framework may not protect them from sophisticated attacks.

Without clarity as to our goals, it is impossible to know if we have achieved them, and, hence, impossible to know how to construct corporate and public policies going forward.

One place to start is by becoming more precise about who, specifically, is the target of the EO effort. The stated target in the EO is critical infrastructure, defined as: “systems or assets, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security or national public health or safety.”

While this definition may seem clear with respect to traditional infrastructures, its application in the cyber context is far more complicated. Cyber systems, including vital military systems, are typically produced using multiple (sometimes thousands) of different entities often located in multiple countries. The systems can be compromised at many different points in this process. So, how far down the supply chain is “critical”?

In addition, one of the defining characteristics of the Internet is its interconnectedness. Does being interconnected with a critical system make you critical from the Framework’s perspective? Does simply providing interconnection make you critical?

Moreover, simply being critical does not mean that a corporate entity has similar structures, economics or security needs as another critical infrastructure. There can be companies with economies of scope and scale that are part of the critical infrastructure and small entities that lack these characteristics but are also critical infrastructure.

While some have asserted that the Framework provides a language for Executives to talk to IT personnel, the most recent draft seems predominantly geared to the technical and may find discussions generated by publicity about the framework very frustrating.

Most senior executives are likely to ask, “Have we ‘adopted’ or are we in ‘compliance’ with the Framework?” They will likely be told it’s impossible to answer these questions clearly and that the goal is to simply “use” the Framework.

A logical follow-up will be, “Well, do we use it?” The likely answer will be that “we do ‘use’ some of it.” Executives may be unsatisfied with such vagueness and may press: “Does using a portion of the Framework constitute ‘adoption’? Does consideration of the Framework constitute ‘adoption’? Can a sector alter the Framework, and does this alteration meet criteria for ‘adoption’? Is it necessary to have the entity’s level of adoption confirmed by a third-party assessor?" And perhaps most predictably and problematically, "Does this lower my liability?"

Indeed, what level of "adoption/use" is required for an entity to qualify to receive the incentives called for in the Order to drive adoption (this will be explored further under question 3)?

Framework drafters have asserted these issues can be addressed by looking to so-called "early adopters." However, highlighting "early adopters" should not be confused as indicating that the Framework is attractive to its target audience. The private sector in general already spends heavily on cyber security and has dramatically increased that spending in recent years. Many organizations have essentially "adopted" the Framework elements long before the Framework, itself, was constructed. Studies suggests 40-50% of private entities can be classified into this "best practices" group.

Early adopters are, almost by definition, those entities for which adopting/using the Framework is the easiest. There is little reason to believe that entities that are already doing a good job of cyber security are very similar to those that are not the non-early adopters, and which, presumably, are the companies we need to be identifying and focusing on.

The true goal of the President's Order is, or at least ought to be, to improve our nation's cyber security. If this is the case, then a listing of entities that were already using the techniques described in the Framework as of the day it is released is fairly meaningless.

The important question is not how many entities are "early adopters" of the Framework on (or soon after) day 1 or even 31. What is important is how many entities that were not using these techniques on day 1 began to adopt them as of day 101, 301, etc.?

In addition, voluntary self-reports from "early adopters" are unreliable indicators of adoption rates or rationales for the rest of critical infrastructure. It is a well-known principle of research methods that voluntary self-report data is among the most unreliable and invalid type of data. Respondents have been shown to routinely bias their reports toward what is socially acceptable or what the investigator desires, while minimizing factors that may make them look bad to the investigators or themselves.

No responsible for-profit entity would rely on such an informal and unsystematic method to assess the success of a new product or service.

Making critical, national security policy decisions based on the least reliable and least valid sort of data is obviously not in our national interest. Relying on this sort of data may well be worse than no data at all, as it may well provide false positives or misleading reports, which, in turn, could result in misguided policies that could have potentially catastrophic effects.

### 3. Has enough work been done on the incentives called for in the EO?

President Obama's Executive Order required several reports on incentives that could be deployed in order to motivate voluntary adoption of the Cybersecurity Framework that NIST was called upon to develop. Presumably, if certain key elements of the NIST Framework were not cost-effective, voluntary adoption of the Framework could be motivated through the deployment of these incentives. Leveraging incentives for resilience and security is also called for in the new "National Infrastructure Protection Plan."

Additionally, as will be discussed further under question 5, there are a wide range of serious cyber attacks, such as the so-called "Advanced persistent Threat" (or "APT"), that are unlikely to be addressed by adoption of the current industry standards in the Framework. Combating these more sophisticated attacks may require substantially greater investment than simple Framework adoption, and, hence, substantially greater incentives may be required.

Under the President's Order, the U.S. Departments of Treasury, Commerce, and Homeland Security were each required to make recommendations on a set of incentives that might encourage voluntary adoption of the Framework. The reports were to include an analysis of the benefits of the incentives relative to their effectiveness. In other words, would the financial benefit offered to the corporation, e.g., an insurance discount, be sufficient to offset the incremental cost so as to motivate voluntary adoption of the security measures in the Framework. A joint GSA-Department of Defense report on the use of security standards in government procurement was also required.

The compressed timeframe for the various incentives reports meant that the incentive reports were due before the initial Framework was released for comment, which meant that the Departments were asked to produce reports on incentives to adopt the NIST Framework, without knowing what the NIST Framework would look like. Perhaps, as a result of this incongruity, the initial incentive reports were vague and tentative.

Various industry groups identified a wide range of market incentives, many based on precedents in other areas of the economy, such as agriculture, environment, aviation, etc., that might be used to offset costs that industry might need to bear in order to take on non-commercial, but national-security-required, cyber defense responsibilities. Among the areas suggested by industry comments and the four government reports were liability incentives, procurement preferences, regulatory forbearance for good actors, patent preferences, streamlined regulation, stimulating the use of the private cyber security insurance market, tax incentives, conditioning government grants on adopting the Framework, advanced technical assistance, access to premium information, creative marketing of security services, and branding advantages.

Many of the incentive ideas had multiple levels of operational adaptability. For example, procurement, liability and insurance incentives could be used to motivate many different types of pro-security behavior.

Following the submission of the various government reports in early spring of 2013, White House National Cybersecurity Coordinator Michael Daniel posted a blog entry enumerating many of the incentive options that the White House planned to consider further. Unfortunately, the incentive development process seems not to have progressed much beyond Mr. Daniel's blog. Indeed, there have been no follow-up reports from the White House or from any other federal entity since Mr. Daniel's August 2013 blog entry.

The President's Order also calls for regulatory agencies to review their current authorities to encourage adoption of the Framework within 90 days of the Framework's February 2014 publication date. However, the Order specifies that this review must also be guided by previous Executive Order Executive Order 12866, which states under Section 1(b) that:

> "(3) Each agency shall identify and assess available alternatives to direct regulation, including providing economic incentives to encourage the desired behavior, such as user fees or marketable permits, or providing information upon which choices can be made by the public…. (and)
>
> "(5) When an agency determines that a regulation is the best available method of achieving the regulatory objective, it shall design its regulations in the most cost-effective manner to achieve the regulatory objective. In doing so, each agency shall consider incentives for innovation, consistency, and predictability, the costs of enforcement and compliance (to the government, regulated entities, and the public), flexibility, distributive impacts, and equity."

To ISA's knowledge, there have been no meetings with industry to substantively explore the cost of implementing the Framework. No timetable exists for considering, let alone deploying, the incentives that might have substantive economic impact on adopting the Framework. Although Administration officials often cite the need for Congress to enact some of the incentives, they have also said that they have no plans to suggest a package to the Congress.

Although NIST was funded to hold 5 nationwide workshops to develop a Framework of aggregated standards and practices, there has been no similar effort to understand the cost to industry so that incentives could be developed to motivate critical infrastructure to voluntarily adopt the Framework. Especially given the fact that the Framework development process itself failed to address the required cost-effectiveness issue, the lack of progress in developing the incentive proposals that industry has made has resulted in a Framework of indeterminate cost and benefit with no added motivation for its voluntary adoption. Thus, it is questionable as to if the Framework effort will result in any significant security beyond what already exists.

### 4. **Are we measuring our efforts appropriately and adequately**?

As the President's Executive Order is historic and precedent setting, it was not realistic to accomplish the deadlines set forth in the Order within one year's time.

Moreover, regardless of the perhaps unforeseen difficulty in resolving core issues, such as what counts as "adopting the Framework," determining if the Framework is cost-effective or not, and identifying how to adapt incentives used in other economic sectors in a cyber security context, there has been a good deal of excellent work done in fulfilling the Executive Order.

Despite this progress, however, both the Executive Order, and the NIST Framework have not been sufficiently tested in order to merit broad scale deployment and implementation at this time.

ISA and entities as diverse as the Financial Services Sector Coordinating Council[vi] and the California State Public Utilities Commission[vii] have each called for a series of pilot, or "beta," tests, which can help clarify some of these outstanding issues and place the Order on a firmer footing for full implementation.

At this point, there has been no baseline data developed against which to measure the cost or effectiveness of the NIST Framework. We have already covered the fact that there is no analysis of the cost-effectiveness of adopting the Framework. Moreover, there is no data presented as to the actual effectiveness (i.e., impact) of the standards and practices suggested by the Framework. Put simply, there has been no data presented that would assure an entity potentially interested in adopting the Framework that by doing so it would be any more secure, let alone secure in a cost-effective manner.

There is much to be encouraged by in the process NIST employed to develop the Framework. However, assuming the product so developed is the appropriate model without systematic testing is problematic.

The Beta Test Proposal, which ISA has spelled out in some detail in its comments on the NIST Framework, is a simple extension of what virtually any sophisticated private sector entity would undertake prior to a full deployment of any new service or product: providers test their offerings with a target group and develop systematic data upon which they make informed decisions and final modifications prior to deployment.

In brief, the proposal is for DHS and the other Sector Specific Agencies charged with implementing the Executive Order to work with their assigned Sector Coordinating Councils to discretely (i.e., non-publicly) target (and then anonymize) a set of organizations that are jointly determined to be prime critical infrastructure targets for which the Executive Order is designed to address. In a slightly more sophisticated version of the model used commonly in the private sector, the audiences would be "segmented' so that conditions at larger targets (and we believe there are large company targets) can be teased out from the conditions effecting smaller entities.

Working together with the target entity on a voluntary basis, the appropriate sector specific agency could assist in implementing the Framework in a jointly determined and agreed upon manner that is appropriate for the volunteering entity. The sector specific agency could provide technical assistance, track costs/benefits and provide incentives to offset costs. From this, the SSA and Sector Coordinating Council could issue a report detailing the above, and which would be anonymized and vetted by the volunteering entity.

The expectation is that such reports would yield hard data about the relative cost-effectiveness of the various elements of the Framework and the ability of the incentives to offset these costs. Based on these metrics, which are currently unavailable, projections can be made for the rest of the community by extrapolation as to what Framework segments are and are not economically feasible.

In addition, this data could provide Congress with currently unavailable, but invaluable, information as to what, if any, additional incentives they need to enact to encourage private sector entities to move beyond their commercial interests and invest in cyber security initiatives that are required for national security purposes, but are not commercially justifiable.

It should also be noted that this testing procedure does not delay current adoption of the Framework. So called "early adopters" can and will continue to use the Framework, and the Government is free to communicate with them to garner whatever voluntary self-report data they choose to provide. Indeed, it is presupposed that this beta testing process would occur in parallel, allowing for simultaneous data gathering from the true targets of the Executive Order, i.e., entities for whom the decision to use the Framework is not so simple on day one, and who need to carefully analyze the costs and benefits of adopting the NIST Framework on a sustained, long-term basis. Measuring effectiveness of achieving our security goals is also called for in the new "National Infrastructure Protection Plan."

### 5. Has the work under the Executive Order addressed the most serious of our cyber threats?

The President's Order candidly describes the potential effects of a serious cyber attack on critical infrastructure in its Section 2 description/definition of critical infrastructure:

> "[T]he term critical infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

As discussed earlier, due to the distributed and interconnected nature of the internet, there is a large universe of companies that can at least theoretically lead experience the massive effect described in the Order if attacked, and, thus, could be considered as targets for Framework deployment. Examples could include small suppliers of critical elements to weapons or public utilities or large entities whose historical economic model does not fit well with the speed of the digital age and cyber attacks.

While some cyber attacks can now be launched with comparatively little technical expertise, attacks generating the magnitude of effects described in the President's Order would likely require sophisticated methods to overcome existing defensive strategies.

The NIST Framework of industry standards and practices largely describes what has come to be called good cyber hygiene. There is general consensus, including some solid research that suggests, that 80% or more of cyber-attacks can be successfully prevented or mitigated by using these techniques.[viii], [ix], [x] However, attacks of the degree of sophistication described in the President's Order would likely fall into the other 10-20% of cyber attacks.

Attacks of this degree of sophistication were once classified as APT (or "APT style") attacks, with APT standing for the Advanced Persistent Threat. APT attacks are generally characterized by an ever increasing and evolving set of attack techniques to compromise a target, often with the attack methods uniquely tailored to address a specific target. The core characteristic of such attacks is that they will continue to evolve until they succeed in compromising the perimeter of the target. Standard defenses, such as anti-virus and intrusion detection systems, will not prevent APT style attacks. In reality, the term APT has become somewhat out-of-date as cyber attacks are growing in increasing sophistication with many commercial attacks now having at least some of characteristics formally associated with the APT.

While this more sophisticated type of attack was at one time confined to governments and major defense integrators, such attacks have become more common over the past few years. What might have been considered a sophisticated attack 5 years ago may have become fairly commonplace 3 years ago and then somewhat dated a year later. Even the recent attack on Target could be considered an "APT-style attack" in that, like APT attacks, it was a multi-dimensional attack that utilized customized, stealthy, malware designed to exploit a vulnerability that the attackers discovered through reconnaissance.

While attackers may initiate an attack using traditional methods, the more sophisticated attackers will elevate their methods as they confront modern defenses until they have successfully compromised their victim.

These sophisticated attackers, including nation-states and nation-state affiliated sources (and increasingly criminal organizations), will not be substantially deterred by the basic hygiene associated with the standards and practices in the NIST Framework.

So, while broad based adoption of the standards and practices outlined in the Framework would clearly be a positive development, policy makers should not assume that such Framework adoption would forestall the sort of sophisticated attack and severe effects described in the President's Order, or even in recent press reports.

For these more sophisticated attacks, deployment of common industry standards and perimeter-based technologies will not prevent them from succeeding. To address the threat described in the President's Order, a more sophisticated cyber defense system needs to be developed.

This more sophisticated system of cyber defense may also require substantially more investment than would be required for the NIST Framework. A study conducted by the Ponemon Institute for Bloomberg in 2012 concluded that protecting critical infrastructure from catastrophic cyber attacks might require as much as a nine-fold increase in cyber defense spending.

Fortunately, there has been substantial work done in the private sector to begin to address this level of threat. However, such techniques were not generally part of the open NIST process.

To address the threat level described in the President's Order, a different process, including a more sophisticated cost-benefit analysis and development of a substantial incentive structure may be required.

## ENDNOTES:

[i] SANS. "SANS NewsBites – Volume XV, Issue: 69." Newsletter. SANS, Aug. 2013. Web. 24 Jan. 2014. <http://www.sans.org/newsletters/newsbites/newsbites.php?vol=15&issue=69>.

[ii] PricewaterhouseCoopers. "The Global State of Information Security: 2008." Rep. PricewaterhouseCoopers, 2007. Print.

[iii] Baker, Stewart, Shaun Waterman, and George Ivanov. "In the Crossfire: Critical Infrastructure in the Age of Cyber War." Rep. McAfee.com. McAfee, 2010. Web. 30 Apr. 2013. <http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf>.

[iv] Domenici, Helen, and Afzal Bari. "The Price of Cybersecurity: Improvements Drive Steep Cost Curve." Rep. Ponemon Institute-Bloomberg Government Study, 31 Jan. 2012. Print.

[v] Starting with workshop 1, final agendas for each workshop can be accessed through the following hyperlinks:
Workshop 1 Final Agenda: <http://www.nist.gov/itl/csd/upload/CSF-April-3-FinalAgenda.pdf>.
Workshop 2 Final Agenda: <http://www.nist.gov/itl/csd/upload/final_agenda_eo_cmu_may29-31_2013.pdf>.
Workshop 3 Final Agenda: <http://www.nist.gov/itl/csd/upload/3rd_cybersecurity_workshop_final_agenda.pdf>.
Workshop 4 Final Agenda: <http://www.nist.gov/itl/csd/upload/Framework_agenda_final_090613.pdf>.
Workshop 5 Final Agenda: <http://www.nist.gov/itl/csd/upload/5th-workshop_Framework-Agendal.pdf>.

[vi] Financial Services Sector Coordinating Council. "Preliminary Cybersecurity Framework Comments." Letter. NIST, Dec. 2013. Web. 24 Jan 2014. <http://csrc.nist.gov/cyberframework/framework_comments/20131213_charles_blauner_fsscc.pdf>.

[vii] California Public Utilities Commission. "Response to the National Institute of Standards and Technology, U.S. Department of Commerce, 'Improving Critical Infrastructure Cybersecurity Executive Order 13636: Preliminary Cybersecurity Framework." Letter. NIST, Dec 2013. Web. 24 Jan. 2014. <http://csrc.nist.gov/cyberframework/framework_comments/20131216_christopher_villarreal_cpuc.pdf>.

[viii] Verizon Enterprise Solutions RISK Team. "2009 Data Breach Investigations Report." Report. *Verizonenterprise.com*. Verizon, 2009. Web. <http://www.verizonenterprise.com/resources/security/reports/2009_databreach_rp.pdf>.

[ix] Verizon RISK Team, et al. "2011 Data Breach Investigations Report." Report. Verizonenterprise.com. Verizon, March 2011. Web. <http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf>.

[x] Verizon RISK Team, et al. "2013 Data Breach Investigations Report." Report. *Verizonenterprise.com*. Verizon, March 2013. Web. <http://www.verizonenterprise.com/DBIR/2013/>.