STRATEGIC INSIGHTS

ASPI

Cybersecurity by executive order

68

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE

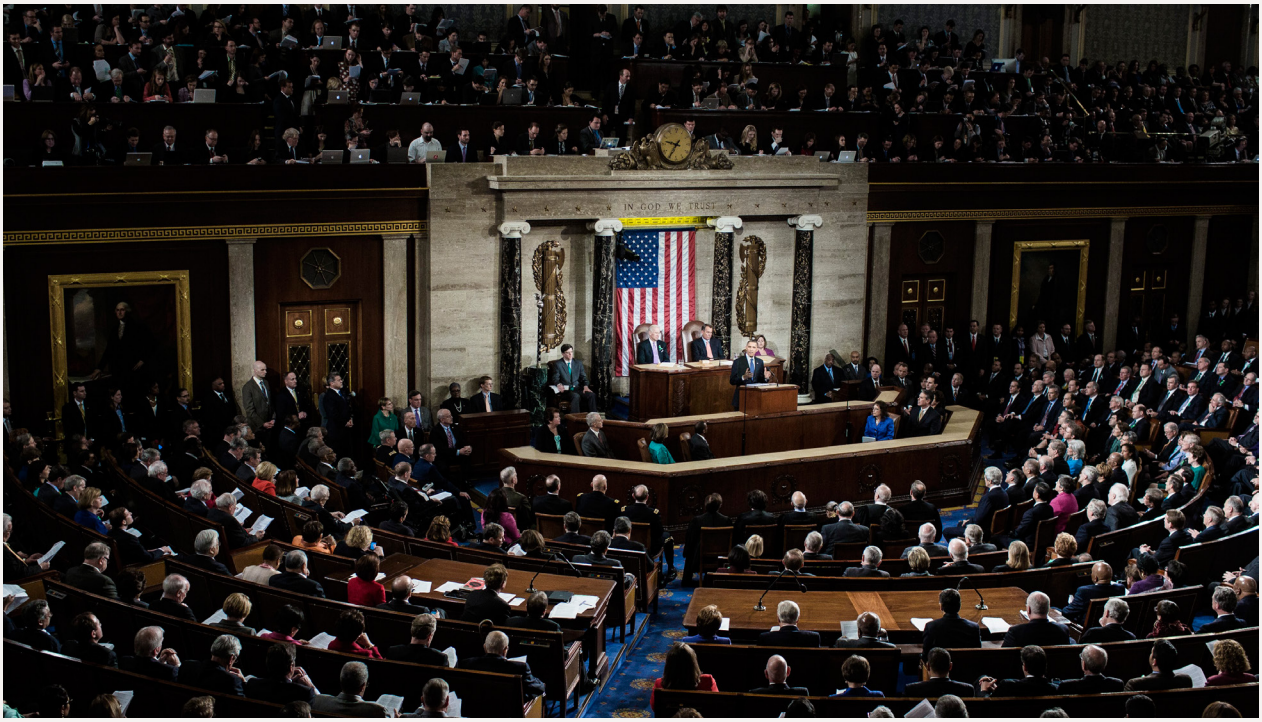
INTERNATIONAL CYBER POLICY CENTRE

Klée Aiken

Executive summary

On 12 February 2014, the US National Institute of Standards and Technology (NIST) released the Framework for Improving Critical Infrastructure Cybersecurity, the flagship accomplishment of the Obama administration's 2013 cybersecurity Executive Order. Just weeks before the White House announced the order, the then Australian Prime Minister Julia Gillard made an equally exciting declaration introducing the Australian Cyber Security Centre (ACSC). One year on, the contrast between the two efforts is stark.

Facing years of congressional inaction on cyber issues, President Obama chose to take executive action on this critical national security issue. Executive Order 13636 set in motion a range of cross-governmental efforts to drive improvements to America's critical infrastructure cybersecurity, with an emphasis on public–private partnerships.



President Barack Obama gives the State of the Union address at the US House of Representatives chamber in Washington, D.C. on 12 February 2013. © T J Kirkpatrick/Corbis

Although legislative malaise continues to mar progress, the US administration's cyber efforts are effective in laying out clear milestones and definitive timeframes to keep the gears of government moving and to measure progress. With the launch of the NIST framework, the merits of the effort will face further scrutiny. But efforts to harmonise priorities across the US Government and the commitment to engaging the private sector will ensure that the US has, at the very least, taken a significant first step forward in critical infrastructure cybersecurity.

Similarly, the ACSC offers Australia a promising road forward to improve public–private partnerships in cyberspace. However, with the 'Coming soon!' sign gathering dust and cyber efforts retreating behind the veil of government, Canberra needs to recommit to cyberspace.

The US and Australia have common interests in developing a robust partnership between the government and private sector to develop whole-of-system cybersecurity. The Obama administration's efforts, while far from perfect, offer critical lessons that the Australian Government can adopt and adapt to improve system-wide cybersecurity and ensure that the ACSC is a successful endeavour. To move beyond political optics, the ACSC must embrace existing best practices, commit to meaningful public–private partnerships, and set a pragmatic forward strategy.

In any truly two-way dialogue on cybersecurity, the private sector must be equal participants. Efforts to streamline security clearances for critical private-sector actors, a dedicated public–private secondment scheme, industry protections, and a collaborative standards process with clear incentives are needed to ensure that public–private partnerships transcend simple lip service. In a sector as dynamic as cybersecurity, it's essential that efforts are underscored by flexibility and resilience and that the private sector is meaningfully engaged in the conversation rather than dictated to.

At the same time, the government must hold itself to higher standards. A clear roadmap for whole-of-government cybersecurity policy is needed to provide direction and offer markers by which to measure success. Coordinating this effort will require that ownership of the policy area is reaffirmed, but also that power remains devolved to the most effective departments and agencies. Fixed deadlines and clearer leadership and coordination will not only improve intragovernmental efforts on cybersecurity, but also provide clarity for the private sector, improving confidence and collaboration.

The ACSC offers the Australian Government a real opportunity not only to demonstrate that it takes cybersecurity seriously, but also to take practical steps to improve whole-of-system cooperation and security. It's up to the current government to be responsible stewards of this effort and transform the ACSC into a truly effective mechanism for intragovernmental and public–private cooperation and collaboration on cyber issues. To do this, the Abbott government should channel the pragmatic steps outlined in the US Executive Order, pre-empt its weaknesses in privacy and liability protection, and put some weight behind the claim that Australia is indeed a regional cyberpower.

Introduction

On 23 January 2013, Prime Minister Julia Gillard announced the creation of the Australian Cyber Security Centre (ACSC) to act as a hub for government cyber efforts. She named 'integrated cyber policy and operations' as one of three national security priorities, and said that the ACSC would act as the node for cooperation and coordination between the government and the critical infrastructure sector and industry partners. This was an ambitious move by the Prime Minister to bring government cyber efforts up to pace with the dynamism of the ever-evolving cyber frontier. It showed that Canberra was serious about whole-of-system cybersecurity.

Just weeks later and only hours before the annual State of the Union address, President Obama signed Executive Order (EO) 13636 *Improving Critical Infrastructure Cybersecurity*. Defiantly admonishing a 'do-nothing' Congress, the President sought to take ownership of the issue and kick-start US cybersecurity efforts that had largely stagnated in the face of partisan bickering. Similar to the Australian Government approach, the Obama administration recognised the critical partnership between the government and the private sector and emphasised the role of government in providing advice and helping to developing effective whole-of-system cybersecurity strategies.

The events of the past year have done nothing but further highlight the importance of robust and resilient cybersecurity measures, but as 2014 rolls on the ACSC has yet to take form and most efforts have slid behind the veil of government discretion. Meanwhile, on the far side of the Pacific, the US National Institute of Standards and Technology (NIST) has rolled out its Framework for Improving Critical Infrastructure Cybersecurity, the flagship effort of the EO, and the Department of Homeland Security (DHS) has launched its Critical Infrastructure Cyber Community C^3 Voluntary Program to build public–private partnerships to help critical infrastructure sectors manage cyber risks.

The US and Australia have a common interest in developing a robust partnership between government and the private sector to develop whole-of-system cybersecurity. Over the past decade, the US Government has slowly developed its response to cyber threats on multiple fronts, and understanding the successes and challenges faced by the US can help Australia develop its own policies. The EO is but one element of the US Government's attempts to build cyber strategies, engage public and private sector players and operationalise policy. While it may be far from perfect, EO 13636 offers critical lessons that can be applied to the Australian context, and if nothing else offers the message that a little bit of executive prerogative can do wonders for cyber policy.

Improving critical infrastructure cybersecurity through an executive order

The Obama administration has long supported a more robust federal approach to cyberspace. Building on the efforts of the previous administration, President Obama commissioned the 2009 Cyberspace Policy Review, established the Cybersecurity Office within the National Security Staff, and appointed a US Cybersecurity Coordinator. But congressional efforts have been stalled since the 2002 *Federal Information Security Management Act*, severely limiting the scope of government activity in this critical national security area. To many, the EO represents a bottom-of-the-barrel solution, conceived from legislative apathy and born constitutionally constrained, but in its implementation the EO has the potential to truly move cybersecurity efforts in the US forward.

Because of the EO's bold rollout in the State of the Union address and the equally politicised response to it, it's important to take a step back and unpack the specific efforts outlined by the order to truly understand its implications. Due to the constitutional separation of powers, the order relies heavily on existing federal authorities and is built principally on already existing programs. In short, EO 13636 is designed to leverage already existing federal regulatory authority to build a framework for voluntary, collaborative cooperation between the US Government and critical infrastructure owners and operators.

Broadly speaking, the directives of EO 13636 can be separated into four general categories; critical infrastructure identification, privacy and civil liberties protection, information sharing, and the Cybersecurity Framework.

Identification of critical infrastructure

The first task of critical infrastructure protection is logically the identification of critical infrastructure. The US Government defines critical infrastructure as 'systems and assets, whether physical or virtual, so vital to the US 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.'[1] Under this metric, the Department of Homeland Security (DHS) identifies 16 sectors as constituting critical US infrastructure.

The EO specifically charges the Secretary of Homeland Security to work with sector-specific agencies to identify specific critical infrastructure vulnerable to cybersecurity incidents that could result in 'catastrophic regional or national effects'. In July 2013, DHS completed its preliminary review of critical infrastructure vulnerable to cyber threats. While specific findings remain confidential under the EO, financial services, telecommunications and energy are seen as the most at-risk sectors.[2] This process of sector identification is updated annually and establishes a baseline for the eventual implementation of the Cybersecurity Framework and other critical infrastructure cyber efforts.

Privacy and civil liberties protection

Privacy and civil liberties protections are often taken as a given under US law, but in the case of critical infrastructure cybersecurity the explicit reiteration of those protections is particularly important. The EO explicitly states that any activities undertaken under the order will incorporate privacy and civil liberty protections based on the Fair Information Practice Principles and other relevant policies. In a way, the emphasis on these protections, most notably the protection of voluntarily submitted information, is meant to assuage the liability concerns of critical infrastructure entities.

One of the most significant limitations of the EO, in comparison to legislative action, is that the effort relies on voluntary participation without specific intellectual property and liability protections. These issues are paramount in the critical infrastructure sector, and many argue that private sector participation will be limited or at the very least abridged without proper protection from litigation and the protection of intellectual property.

Information sharing

Timely and effective information-sharing is a pressing issue when it comes to protecting critical infrastructure. It also presents some of the largest hurdles to national cybersecurity efforts, including the classification of critical information and concerns about corporate liability and intellectual property. Broadly, the EO calls on the Attorney General, the Secretary of Homeland Security and the Director of National Intelligence to increase the 'volume, timeliness, and quality of cyber threat information shared with US private sector entities'. On a more practical level, this directive involves the expansion of existing government information-sharing programs and the establishment of a cross-sector consultative process to inform and coordinate improvements to critical infrastructure cybersecurity.

EO 13636 builds on the continuous evolution of the Department of Defense Cybersecurity/Information Assurance (CS/IA) Program, which worked with the National Security Agency to share cybersecurity best practices and cyber threat information between the government and defence contractors. In July 2012, the CS/IA Program was permanently moved to DHS to allow it to expand to other critical sectors. The EO calls for this program, now called Enhanced Cybersecurity Services, to be expanded to all critical infrastructure sectors. To facilitate the program's expansion and improve its functionality, the order lays out several key initiatives, including the identification and dissemination of cyber threat indicators, expedited processing of security clearances for select critical infrastructure personnel, and the expansion of private-sector expert secondment into federal agencies.

Cybersecurity Framework

The flagship of the EO is the creation of a cybersecurity framework and the expansion of existing critical infrastructure initiatives to implement the framework. This effort begins with the creation of cybersecurity technical standards by NIST.

The EO established a rather ambitious timetable for NIST to create a comprehensive cybersecurity framework. Using existing federal practices on standards development, including cross-sector consultation and public comment periods, NIST completed its preliminary framework in October 2013 and published Version 1.0 of the Framework for Improving Critical Infrastructure Cybersecurity on 12 February 2014. Due to the constraints of the EO, the best practices and standards outlined in the framework are only voluntary, resulting in mixed expectations as to their worth. At the same time, senior administration officials extol the voluntary nature of the program as encouraging the participation of the 'widest possible set of stake holders' and making the standards 'much more likely to be adopted quickly and implemented fully'.[3]

The NIST Framework for Improving Critical Infrastructure Cybersecurity was developed with an awareness of its inherent limitations as a voluntary exercise, and NIST sought to leverage industry collaboration to ensure the full utility of the final framework. The framework is framed as a roadmap to complement, rather than to replace, cybersecurity efforts, and administration officials have taken to calling it a 'living document', emphasising its flexibility and customisability.

Specifically, the framework identifies five core functions and subdivides each into categories matched with an existing catalogue of standards, guidelines and practices. The five core areas—Identify, Protect, Detect, Respond, Recover—are designed to address the high-level, strategic management of cybersecurity risks, while 'framework profiles' and 'implementation tiers' allow a common language to align organisational cybersecurity with the framework's guidelines.

The framework holds itself to rather lofty goals, especially given its reliance on existing standards, regulations and best practices. By providing a common language and a standardised mechanism to inform the cybersecurity decisions of critical infrastructure organisations, it presents itself as an enabler of economies of scale. NIST suggests that, in doing so, it will catalyse cyber 'innovation and development of effective products and services that meet identified market need'.[4]

In parallel with the development of the NIST Cybersecurity Framework, partner federal agencies are taking steps to use existing partnership programs to facilitate the adoption of the framework. Those steps include:

- the establishment of the DHS Critical Infrastructure Cyber Community C^3 Voluntary Program to support the adoption of the framework
- the utilisation and expansion of existing Critical Infrastructure Partnership Advisory Council structures to include cyber matters
- leveraging the buying power of the US Government by incorporating security standards into acquisition and contracting
- ongoing collaborative review and updating of the framework, including a NIST Roadmap for Improving Critical Infrastructure Cybersecurity outlining efforts to develop Version 2.0 of the Cybersecurity Framework.

Debilitating shortcomings?

Overall, the Obama cyber EO left many analysts wanting more. The grandiose promise in the State of the Union address suggested an overarching federal effort to combat hackers and foreign corporate cyber-espionage on top of moves to secure critical infrastructure, whereas the effort itself is much more narrowly defined. The reality is that the EO is stymied as much by a lack of ambition as by constitutional constraints.

Criticisms of the EO range from basic concerns about the constitutional separation of powers and broader concerns about government regulation to more pointed criticisms highlighting the weakness of voluntary participation and questioning the value of cutting and pasting already existing policies. While we'll leave the politicised debate over the separation of powers and the role of government regulation and standards in the economy to the politicos, there are many criticisms of the EO as a means to improve cybersecurity that must be examined.

A particularly stinging criticism of the administration's cyber effort warns that, when dealing with a dynamic and transformative field such as cyber, business-as-usual policymaking simply can't keep pace. The cyber effort has received broad criticism: it's been called 'toothless', likened to a step backwards[5], and had its provisions lambasted as flawed, coercive and unrealistic.[6] More diplomatically, Jason Healey of the Atlantic Council has called the EO the latest 'small step … in a fifteen-year parade', offering a 1998 Presidential Directive as evidence of Washington's snail's pace.[7] After examining documents such as the 2009 National Infrastructure Protection Plan or any number of past cyber efforts, one would be forgiven for thinking that many of EO 13636's provisions should already be in place. Even without a historical perspective, it's clear that the EO heavily recycles existing policy: it's fully reliant on existing authorities, its information-sharing ambitions are based on well-known government – critical infrastructure apparatus, and even the NIST Cybersecurity Framework acts primarily as an index to existing standards and best practices.

These shortcomings can be placed squarely on the format of the action. Regardless of White House intentions, the use of an EO rather than legislation severely limits its utility. The constitutional limitations of the order are unfortunately most evident in the most critical provisions—those relating to privacy and providing incentives.

Although the EO pulls extensively on existing privacy and civil liberties protection, for industry the protection of business and economic interests is paramount. Industry requires direct and detailed protections of privacy, liability and intellectual property and protections from reputation costs if it is to share information. While cybersecurity is widely accepted as an important issue, without the proper protections the business case concerning voluntary contributions is heavily skewed towards nonparticipation. Congressional action alone can provide the level of protection to truly make the EO's programs a reasonably viable option for business.

Ongoing problems with federal cyber efforts further reinforce criticisms that will become increasingly politicised. On 4 February, Senator Tom Coburn established an early stake in the battle, releasing *The Federal Government's track record on cybersecurity and critical infrastructure*. Outlining numerous vulnerabilities in government cybersecurity efforts and emphasising an estimated US$65 billion price tag, the report is in many ways a political prop, but that isn't to say that some of its conclusions are unfounded.

In fact, just two days after the 2013 State of the Union address, the non-partisan Government Accountability Office (GAO) released an equally damning report auditing national cybersecurity strategy, roles and responsibilities. Aptly titled *National strategy, roles, and responsibilities need to be better defined and more effectively implemented*, the report supported many criticisms of the EO, finding many government efforts lacking and progress largely incremental. The report recognised the many cyber efforts across the government, but highlighted that, while those efforts might address specific aspects of cybersecurity, an overarching strategy was needed—a void the EO clearly doesn't fill.

In full fairness, the review didn't include the provisions of the EO, and the order does indeed address some pressing concerns of the GAO. Specifically, the EO expands DHS cybersecurity efforts to all critical infrastructure, addresses the issue of private-sector security clearances, and directly attempts to improve information sharing. Unfortunately, there's no evidence that the EO will accelerate the glacial pace noted by the GAO. And, while the order does task agencies to act, there's little in the way of substantive additional role defining or strong metrics to measure progress.

Moreover, as early as July, budget constraints led to scaled-back DHS critical infrastructure cybersecurity conferences and training sessions. A recent DHS Inspector General's report has found the National Protection and Programs Directorate's government cyber information-sharing efforts lacking and situational awareness capabilities underdeveloped. Such findings don't bode well for the implementation of the President's cyber initiatives.

With the completion of the NIST's final framework, the EO will be likely to re-enter the political sphere. In a statement releasing the Cybersecurity Framework, President Obama went so far as to directly call out Congress to act on cybersecurity—a move that will certainly ruffle feathers. Even before the release, the House Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies marked up House Resolution 3696: National Cybersecurity and Critical Infrastructure Protection Act of 2013 and passed it on to the House Committee on Homeland Security. This is surely not the last in a bevy of efforts to come in response to both the NIST framework and the scrutiny of private cybersecurity following very public data breaches at Target and Neiman Marcus.[8]

With clear structural challenges, menacing cyber threats, budget battles and a political bloodbath ahead, the outlook for the EO and the NIST framework appears grim. However, with public–private partnerships as the cornerstone of the effort, the NIST framework packs a much larger punch than its detractors may expect.

A cyber 'turning point'

Instead of allowing limitations of executive power to stymie the Cybersecurity Framework, NIST effectively engaged the private sector under the rubric of continuous evolution to establish what truly could be a significant starting point for improving critical infrastructure cybersecurity.

EO 13636 can't be judged fairly without its corresponding Presidential Policy Directive on Critical Infrastructure Security and Resilience (PPD-21). This document, while itself certainly far from perfect, provides a more detailed look into the efforts outlined

in the EO. PPD-21 offers strategic imperatives, defines roles and responsibilities and outlines more detailed implementation measures than those in the order.

PPD-21 offers three strategic imperatives to guide federal efforts: first, to 'refine and clarify' US Government functional relationships; second, to identify baseline data and systems requirements for effective information exchange; third, to implement integration and analysis functions for critical infrastructure planning and decision-making. The directive also offers a clear timetable for action with six milestones to guide federal efforts, ranging from 120 days to develop a clear guide to federal cyber responsibilities and primary points of contact for the private sector to the formation of a National Critical Infrastructure Security and Resilience Research and Development Plan by 2015. Although executive limitations remain, clear milestones offer basic metrics to measure progress and guide individual federal agencies. This helps to ensure steady progress, and bureaucratic momentum is a powerful thing when it comes to government.

The NIST Cybersecurity Framework illustrates the operationalising of the EO and presidential directive and has already received praise from industry. The US Chamber of Commerce has commended NIST's efforts to work with business[9], the Financial Services Roundtable applauded the framework as a 'positive step'[10], and Internet Security Alliance President Larry Clinton has described the process as on the 'right track', praising the voluntary nature of the framework.[11] While support for Version 1.0 of the NIST framework has been tempered by calls for legislation to fully empower cyber efforts, primarily in regard to incentives, the consensus is positive. This is no surprise, or accident, as collaboration was a critical component to ensure the voluntary implementation of the standards.

In fact, the NIST framework has been empowered by removing the hammer of regulation from the process and emphasising voluntary measures. Without the impetus to create standards, the framework avoids a one-size-fits-all approach, building in the flexibility needed to remain nimble in the face of a rapidly evolving threat landscape. This approach also intentionally emphasises market-driven adoption, which is both favoured by industry and more welcoming to innovation.

While there's no explicit enforcement mechanism, standards elicit indirect enforcement. With liability a primary concern for business, the legal repercussions of noncompliance with even voluntary standards could be severely damaging if a cyber-incident were to occur. The GAO found this concern to be a clear motivation for the incorporation of even voluntary standards[12]—a view echoed by former DHS Deputy Undersecretary for Cybersecurity Mark Weatherford, who has emphasised, albeit disapprovingly, the potential legal ramifications for noncompliant organisations.[13] With recent high-profile cyberattacks in the US, this driver will be even stronger.

Moreover, with support from the DHS National Protection and Programs Directorate, the NIST standards provide an important tool for smaller critical infrastructure owners and operators who can use the framework to develop cybersecurity measures where individual budgets would not otherwise allow it. While some argue that the program will do little to combat higher spectrum threats, the assistance that the framework and government implementation programs such as C^3 provide to smaller companies is vital for increasing whole-of-system security. As a senior administration official put it, 'In cybersecurity, the more systems we secure, the more secure we all are.'[14]

While talk of a 'turning point' or 'first step' mightn't be the revolutionary changes some had hoped for, when it comes to government the EO and the NIST framework can be game-changers. The critical point in this isn't in their creation, but in their purposeful integration into a long-term roadmap with marked goals. Calling the Cybersecurity Framework 'Version 1.0' may suggest that it's incomplete, but is in fact a recognition of the continuous, customisable and flexible characteristics necessary for cybersecurity.

The key for the future is the Roadmap for Improving Critical Infrastructure Cybersecurity, launched with the NIST Cybersecurity Framework. The roadmap not only ensures a clear trajectory for government efforts but keeps the feet of bureaucracy to the flame. It ensures continued collaborative efforts to not only formulate Version 2.0 of the framework, but also to address major plot holes.

Focused on development, alignment and collaboration, the roadmap strikes an ambitious agenda of practical steps forward. Work on issues such as 'automated indicator sharing' (to improve the sharing of actionable threat data) and programs to increase the national cybersecurity workforce to overcome the shortage of cyber experts ensure that the practical groundwork for the NIST Cybersecurity Framework will be laid. The planned hand-off of the standards process to an independent non-government organisation further reinforces the public–private essence of the program and will help to ensure the long-term alignment of standards and practices domestically and internationally.

Even before the NIST roadmap was launched, federal departments had already taken promising, progressive action to improve cybersecurity. DHS released an updated National Infrastructure Protection Plan in December 2013, and in November the Department of Defense published a final rule to improve supply-chain security.[15] The Defense Department has also issued an interim rule to update the Defense Federal Acquisition Regulation Supplement[16], the Pentagon's General Services Administration announced broad acquisition cybersecurity and resilience recommendations in January 2014[17], and the Office of Management and Budget made cybersecurity one of 14 cross-agency performance priority goals in November.[18] This activity, while not headline grabbing, all helps to move federal cybersecurity forward.

Legislative action remains critical for the future, but keeping the process going has established the foundations and the ball is now in Congress's court. Issues such as privacy and liability protection will undoubtedly require action on Capitol Hill. Federal incentives to augment market drivers will need congressional support as well. With continued progress by the executive, pressure from within Washington and from the business community will mount. Clearly laying out options for Congress, such as the August 2013 release of potential incentive schemes, will make inaction increasingly untenable.

Are the EO's shortcomings debilitating? While the gap between political optics and reality sparked some kneejerk reactions, since the gears of government have begun to turn the consensus in Washington has largely settled on tentative praise, with calls for congressional action. Over the long term, however, these measured steps have the potential to snowball into more promising and integrated action. Baby-steps in the field of cybersecurity aren't nearly sufficient, but even if those efforts do nothing more than further bolster the conversation in boardrooms and on the Hill, the momentum gained by them is critical. And, if a touch of optimism is acceptable, this effort is poised to lead to much more than simple conversation.

Lessons for Australia

The US offers Australia an ideal laboratory from which to gather critical lessons on cybersecurity. An understanding of the strengths and weaknesses of President Obama's cyber efforts and the context in which they were born will allow the Australian Government to garner best practices and bypass clear barriers. Allowing for the differences between the two countries' political systems, Australia should leverage this opportunity to study Washington's policy and adapt its tenets to build an even more robust and efficient cyber policy, which could in turn offer best practices to the international community.

In many ways, criticisms of the ACSC mirror those of EO 13636. Some charge that, while the centre offers great optics, continuing separate budgets and divisions between policy responsibility and the capabilities to act mean that it simply represents a rebranding of existing policy. While many of those charges may have merit, the ACSC is still evolving and retains the potential to meet its billing. It's up to the current government to be responsible stewards of this effort and transform the ACSC into a truly effective mechanism for intragovernmental and public–private cooperation and collaboration on cyber issues. To do this, the Abbott government should channel the pragmatic steps outlined in Obama's executive order, pre-empt its weaknesses in privacy and liability protection, and put some weight behind the claim that Australia is indeed a regional cyber power.

A strong base built on strong existing policy isn't a negative characteristic in private–public partnerships, which rely heavily on familiarity, trust and habit. To ensure a fluid transition, the ACSC, like the EO, should embrace existing best practices for those partnerships and avoid creating cleavages based on political convenience. Programs such as the Trusted Information Sharing Networks (TISN) have a strong track record, and it would be counterproductive to simply sever strong working relationships. The government must lay out a clear transition plan that incorporates these types of programs into the ACSC.

The new centre provides a great opportunity to highlight the increasing importance of cybersecurity and can have a real benefit in integrating government and private-sector efforts. However, success is unlikely without pragmatic base-level steps to facilitate partnerships. EO 13636 offers some easy-to-implement methods that can provide immediate benefits:

- *Security clearances*: To have a truly two-way dialogue on cybersecurity, the private sector must be incorporated as equal participants. To improve information sharing and, more importantly, to allow the dissemination of critical cyber threat information in real time, Canberra must make a concerted effort to identify appropriate critical infrastructure personnel and expedite the processing of the necessary security clearances. While dealing with sensitive information will always pose a challenge, establishing practised lines of communications will not only improve dissemination of critical information, but also prompt private enterprises to be more forthcoming with their own intelligence.
- *Secondment*: Trust is critical to productive public–private partnerships and interoperability. Temporary secondment of private-sector experts into government benefits both sides of the relationship by infusing private-sector expertise into government functions and helping to translate the inner workings of government for the private sector. By building understanding and dialogue on both sides of the relationship, the government and private sector can more suitably align, or at least understand, each other's concerns, interests and priorities. Secondments are a clear avenue for relationship-building and are a productive good-faith effort that indicates the government's willingness to put substance behind its rhetoric about public–private partnerships.

  Moreover, secondments can help to create fluid working relationships in which collaboration becomes the habit rather than the exception. Government secondment programs can help to build lasting networks between key actors in government and industry and, more importantly, between businesses' representatives. Businesses are naturally hesitant about openness with competitors, so it's up to the government to build an environment in which strong, mutually beneficial working relationships can be established. Such efforts are integral to building the trust that will allow substantive whole-of-system cybersecurity efforts to be viable.

The ACSC must also be backed by clear policy guidelines and protections for the private sector. Canberra needs to provide a clear timeline for the development of standards that incorporate full industry participation:

- *Standards*: The NIST Cybersecurity Framework provides a common language and mechanisms to direct the more practical side of public–private cooperation. Standards provide baseline metrics to evaluate cybersecurity and define parameters to guide private-sector cyber efforts. They also provide clarity and a common ground to ensure basic compliance and to frame government–business and business-to-business collaboration.
- *Engagement*: It's vital that the private sector have an ownership stake in the standards process. The NIST framework process used numerous workshops, webinars, informal sessions and other engagement strategies, earning praise as 'one of the better examples of public–private sector cooperation'.[19] By fully engaging stakeholders throughout the process, NIST has been able to leverage existing best practices and tailor its approach to maximise applicability while avoiding a top-down mandate approach that would severely hamper its impact as a voluntary standard. Cybersecurity must be a partnership between government and the private sector and must be built on engagement rather than policy dictation.
- *Industry protections*: Without the political limitations of the EO, efforts in Australia can overcome the most striking weaknesses of the order—privacy and liability protections. Legislating barriers to the misuse of shared information and protections for proprietary information, privacy, liability and reputation will help industry to balance the costs and benefits of participation. As the government develops its cyber information-sharing schemes, it should actively consult with the private sector to ensure that appropriate protections are put in place to make information-sharing a positive joint effort, rather than a risk for the participants.

- *Marketing participation*: It's not enough for government to remove barriers to cooperation on cybersecurity—the ACSC must also foster an environment that incentivises business participation. For the private sector, participation in a national cybersecurity effort is a business decision that comes with real costs, so the government must ensure clear returns for the sector's participation. There's no reason for businesses to invest in the process if the program doesn't produce tangible cybersecurity benefits. The ACSC must ensure that private-sector investment and information-sharing reduce businesses' cyber risks by designing a forum for real dialogue between government and business as well as among business participants. The forum should be a venue for sharing threat information and disseminating best practices, rather than a mechanism for one-way consultations and information gathering.
- *Incentives*: In instituting cybersecurity standards and bulking up partnerships, cyber policy should favour incentives over regulations. While regulation has its place in ensuring compliance, well-designed incentives can spur innovation and ownership in whole-of-system security, rather than mere compliance. Government should use its full arsenal to bolster private-sector cybersecurity. In the US, DHS, Commerce and Treasury guidance released under the EO offer a buffet of options for consideration. Canberra should also consider those options, including cybersecurity insurance, grants, process preference, liability limitation, streamlined regulation, public recognition, rate recovery for price-regulated industries, and cybersecurity research and development.[20] Alongside considering and adapting these options, the Prime Minister should institute an internal review to develop unique and innovative incentive methods designed for the Australian context.

Clarity will be the lynchpin for the success of government interaction with the private sector on cybersecurity. While the aim of the ACSC is to provide a one-stop government shop for cybersecurity, a lack of substantive proposals to build partnerships and the ambiguity surrounding its launch have dulled its impact:

- *Deadlines*: While the ACSC board (led by the Secretary of the Attorney-General's Department) may have begun meeting, the uncertainty surrounding the launch of the centre has led to confusion, if not indifference, outside Canberra. As EO 13636 did, the government should organise a timetable of hard deadlines and performance measures. A clear timeframe for the launch of the centre, standards creation and other cyber efforts provides not only a framework to measure progress, but certainty for those outside of government to formulate their own cybersecurity strategies and engagement plans.

  For private enterprises to buy into government cybersecurity efforts, the government must commit to meeting its targets. The collapse of the 2011 Cyber White Paper and continued timing challenges for the ACSC have seriously degraded confidence in government cyber plans. Canberra must recommit to a clear roadmap and be vigilant in ensuring that timeframes are met and that the government becomes a reliable partner for business.
- *Leadership and coordination*: Lack of clear leadership is also of concern for outside actors and a major barrier to effective cross-departmental work on the issue. With the Attorney-General's Department taking responsibility for the centre, while capabilities lie primary within Defence and policy is driven by the Department of the Prime Minister and Cabinet (PM&C), there's far too much ambiguity in Australian cyber governance. In an area in which essentially all departments have an interest, a clear chain of responsibilities is critical for the internal workings of government and paramount for government collaboration with outside partners.

  If the government wants to be taken seriously on cybersecurity issues, it must show that it has firm control of the policy space. As the supporting agency for the Prime Minister, PM&C should take ownership of this effort to highlight the government's prioritisation of the issue. While stewardship of cybersecurity has floundered under existing arrangements, a dedicated effort to truly establish the department as the government leader for cyber policy and a consolidation of expertise within the department will go a long way to improve whole-of-government cyber efforts.

  Although strong cyber leadership needs to be established to shape whole-of-government strategy, individual departments have a strong stake in the area and are often better positioned to engage within their domains. A clear delineation of roles and responsibilities for other government departments must also be established to mitigate interdepartmental friction and to

leverage each department's particular expertise and capabilities while avoiding inefficient and duplicated efforts. A position mirroring the White House Cybersecurity Coordinator should be created to coordinate such efforts and be the main point of contact for the private sector.

The ACSC offers real potential to bring together government cyber efforts, as well as to be a global model for public–private cybersecurity cooperation. While significant effort is required to fulfil such aspirations, an openness to learning from other national efforts in cyberspace, including EO 13636, and a willingness to back optics with action can lead to a truly robust Australian whole-of-system cybersecurity effort.

Notes

1 Critical Infrastructure Protection, 42 USC § 5195c.

2 McAfee 2013, *EO 13636: Improving Critical Infrastructure Cybersecurity*, www.mcafee.com/au/resources/solution-briefs/sb-eo-13636-cybersecurity.pdf.

3 The White House 2014, *Background briefing on the launch of the Cybersecurity Framework*, Washington DC.

4 National Institute of Standards and Technology (NIST) 2013, *Improving Critical Infrastructure Cybersecurity Executive Order 13636: Preliminary Cybersecurity Framework*, NIST, Washington DC.

5 Gerry Smith 2013, 'Obama's cybersecurity order weaker than previous proposals', *Huffington Post*, 12 February, www.huffingtonpost.com/2013/02/12/obama-cybersecurity-state-of-the-union_n_2669941.html.

6 Paul Rosenzweig, David Inserra 2013, 'Obama's cybersecurity executive order falls short', *The Heritage Foundation*, 14 February, www.heritage.org/research/reports/2013/02/obama-s-cybersecurity-executive-order-falls-short.

7 Jason Healey 2013, 'Presidential cyber direction looks quite familiar', *Atlantic Council*, 12 February, www.atlanticcouncil.org/blogs/new-atlanticist/presidential-cyber-direction-looks-quite-familiar.

8 Elise Hu 2014, 'Lawmakers look to prevent more target-sized data breaches', *All Tech Considered*, 4 February, www.npr.org/blogs/alltechconsidered/2014/02/04/271448328/lawmakers-look-to-prevent-more-target-sized-data-breaches.

9 Ann M Beauchesne 2014, *US Chamber statement on Cybersecurity Framework*, US Chamber of Commerce, www.uschamber.com/press-release/us-chamber-statement-cybersecurity-framework.

10 Financial Services Roundtable 2014, 'FSR applauds release of NIST Cybersecurity Framework', *Financial Services Roundtable*, http://fsroundtable.org/fsr-applauds-release-nist-cybersecurity-framework/.

11 Jason Miller 2014, 'White House cyber framework focuses on flexibility, risk for critical infrastructure providers', *Federal News Radio*. 12 February, www.federalnewsradio.com/473/3561719/White-House-cyber-framework-focuses-on-flexibility-risk-for-critical-infrastructure-providers.

12 Government Accountability Office (GAO) 2013, *National strategy, roles, and responsibilities need to be better defined and more effectively implemented*, GAO, Washington DC.

13 Drew Amorosi 2013, 'Interview: Mark Weatherford and cybersecurity for critical infrastructure', *Infosecurity Magazine*, 6 November, www.infosecurity-magazine.com/view/35479/interview-mark-weatherford-and-cybersecurity-for-critical-infrastructure/.

14 The White House 2014, *Background briefing on the launch of the Cybersecurity Framework*, Washington DC.

15 Government Printing Office 2013, *Federal Register*, 18 November, Government Printing Office, Washington DC.

16 Government Printing Office 2013, *Federal Register*.

17 Department of Defense 2014, *GSA and DoD announce acquisition cybersecurity and resilience recommendations*, NR-054-14, Department of Defense, Washington DC, 3 February, www.defense.gov/Releases/Release.aspx?ReleaseID=16510.

18 Sylvia Burwell 2013, *Memorandum for the heads of executive departments and agencies*, 18 November, White House, Washington DC.

19 Eric Chabrow 2014, 'On deck: the Cybersecurity Framework', *GovInfo Security*, 8 February, www.govinfosecurity.com/on-deck-cybersecurity-framework-a-6488?CA.

20 Michael Daniel 2013, 'Incentives to support adoption of the Cybersecurity Framework', *The White House Blog*, 6 August, www.whitehouse.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework.

Acronyms and abbreviations

ACSC	Australian Cyber Security Centre
CS/IA Program	Cybersecurity/Information Assurance Program (US)
DHS	Department of Homeland Security (US)
EO	executive order
GAO	Government Accountability Office (US)
NIST	National Institute of Standards and Technology (US)
PM&C	Department of the Prime Minister and Cabinet

Important disclaimer

About the author

Klée Aiken joined ASPI's International Cyber Policy Centre in November 2013 where he works on international and domestic cybersecurity issues. Prior to joining the team, Klée spent several years working in DC, serving a stint in the think tank world before taking a position as an Analyst with a small international consulting firm. Klée holds a Master's degree in International Relations from the Universiteit van Amsterdam in the Netherlands.

About Strategic Insights

Strategic Insights are shorter studies intended to provide expert perspectives on topical policy issues. They reflect the personal views of the author(s), and do not in any way express or reflect the views of the Australian Government or represent the formal position of ASPI on any particular issue.

ASPI
Tel +61 2 6270 5100
Fax + 61 2 6273 9566
Email enquiries@aspi.org.au
Web www.aspi.org.au
Blog www.aspistrategist.org.au