Input to the Commission on Enhancing National Cybersecurity

Response to RFI
Issued August 10, 2016

Prepared for:
Department of Commerce
National Institutes of Standards and Technology
The Commission on Enhancing National Cybersecurity
Date: September 9, 2016

Submitted By:
Waverley Labs, LLC.
PO 213, Waterford, VA 2097
www.waverleylabs.com
Juanita Koilpillai - Technical POC
571-246-6182
jkoilpillai@waverleylabs.com
SAM Certifications - WOSB
Other Federal Agencies – DHS S&T is funding the Open Source SDP
http://www.waverleylabs.com/

Partners:

AOC

Cloud Security Alliance

This response includes data that shall not be disclosed outside the Government and shall not be duplicated, used or disclosed in whole or in part – for any purpose other than to evaluate this quotation. This restriction does not limit the Government's right to use information contained in this data if it is obtained from another source without restriction. The data subject to this restriction are contained in sheets (insert numbers or other identification of sheets)

Input to the Commission on Enhancing National Cybersecurity - Comments

Critical infrastructure is by nature fragile and prone to instabilities inherent in its design. The connectivity, the interconnections and the built-in vulnerabilities for these systems to be stable are what makes it critical. The commercial air transportation system is fragile because of its important hubs, the power grid is weakened by its substations and transmission lines that handle more than their share of connectivity, and the monoculture Internet is prone to malware because of its many connections and the ability of the malicious code to traverse the globe with tremendous speed. It is this structure in the form of network connectivity that renders critical infrastructure vulnerable. It is our opinion that innovation is need to overcome the growing risk and complexity of Cybersecurity.

Our solution focuses on securing these connections and strengthening the underlying structure rather than adding to the instability of the systems by using a novel concept called the Software Defined Perimeter (SDP). SDPs protect critical infrastructure from the top OWASP attacks (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project), all network-based attacks, credential theft, man-in-the-middle attacks and vulnerable code.

The SDP is a new approach to cyber security that mitigates all network-based attacks. It protects both legacy critical infrastructure/IT assets and cloud services of all classification levels. It works by hiding critical infrastructure/IT assets within an undetectable, invisible, black cloud, whether the assets are on-premise or in a public or private cloud, a DMZ, a server in a data center, or even inside an application server.

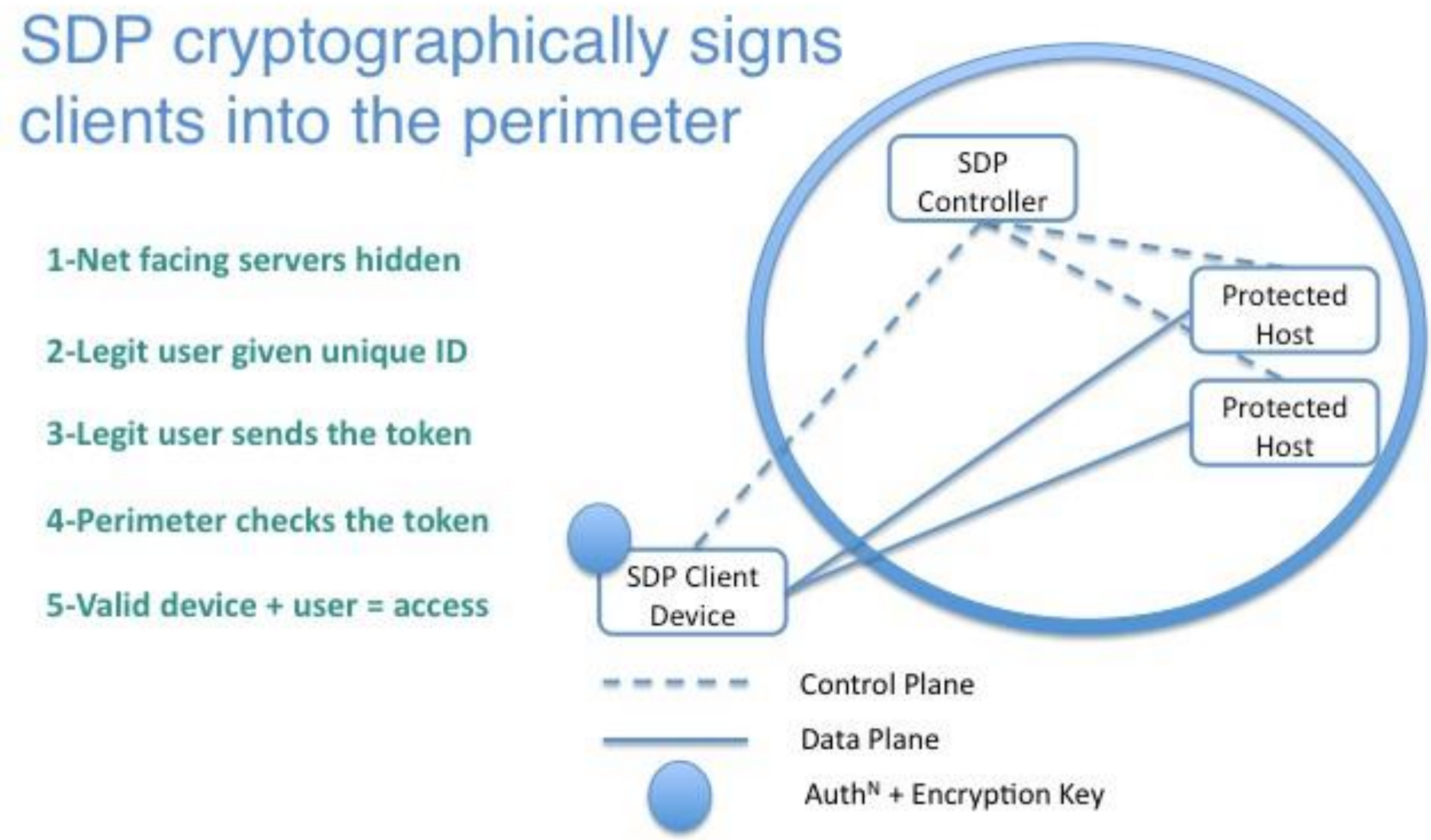
SDP uses a combination of tried and true security protocols that were previously unconnected until the Department of Defense (DoD) announced them working in concert. The Cloud Security Alliance adapted the generalized DoD workflow but modified SDPs for commercial use and made it compatible with existing enterprise security controls. Where applicable, SDP has followed NIST guidelines on cryptographic protocols and securing applications in the cloud.

DHS is now funding the development of an open source version of the SDP for both public and private organizations to defend against distributed denial of service (DDoS) attacks. We have developed an open source reference implementation (http://www.waverleylabs.com/open-source/) of this new security architecture to facilitate wide-spread adoption and shore up our nation's critical infrastructure much faster than is currently trending.

The principles behind SDPs are not entirely new. Software Defined Perimeter (SDP) offers a radically new approach to protecting 'connected' applications that is more affordable and effective as less manpower is required for support. The Software Defined Perimeter, if implemented as specified, deems applications critical infrastructure in the cloud and on-premise impenetrable.

The Software Defined Perimeter architecture and associated components are ***evolutionary*** in that they build upon known controls such as the 'need to know' access model verified in the DoD, device verification proven by NSA and Mutual Transport Layer Security promoted by NIST. Multiple organizations within the DOD and Intelligence Communities (IC) have implemented a similar network architecture based on authentication and authorization prior to network access. Typically used in classified or high-side networks (as defined by the DoD), every server is hidden behind a remote access gateway appliance to which a user must authenticate before visibility of authorized services is available and access is provided. SDPs maintain the benefits of the need-to-know model but eliminate the disadvantages of requiring a remote access gateway appliance. However, these implementations fall short.

The Software Defined Perimeter is also ***revolutionary*** in that it extends the protection to the perimeter that is changing with the advent of mobile devices and the Internet of Things (IoT). SDPs require endpoints to authenticate and be authorized first before obtaining network access to protected servers, and then, encrypted connections are created in real time between requesting systems and critical infrastructure.



SDP cryptographically signs clients into the perimeter

1-Net facing servers hidden

2-Legit user given unique ID

3-Legit user sends the token

4-Perimeter checks the token

5-Valid device + user = access

A. Current and future trends and challenges in the selected topic area

a. Progress being made to address the challenges;

Today’s approach to security is IP-based, and connections are allowed before authorizing and authenticating them. This inherent flaw in our thinking forces activities to focus on securing and hardening machines, gathering massive amounts of data for threat intelligence and creating large incident response teams that despite their talent cannot keep up with securing the infinite connections that happen on a day-to-day basis. This strategy has led to the following trends.

i. Organizations are forced to seek new, faster and smarter point solutions to new and existing threats

ii. Standards bodies are furiously expanding and formalizing security controls that cost a lot of money to not only understand but to implement

    iii. The Cloud-first strategy in the Federal Government has forced consolidation of servers and networks, but systems are still largely insecure

b. The most promising approaches to addressing the challenges;
The release of the SDP Specification by the Cloud Security Alliance (https://cloudsecurityalliance.org/group/software-defined-perimeter/) and bespoke implementations of the specification by large companies like Coca-Cola, Mazda, and Google are starting to take hold. The Department of Homeland Security has funded an open source reference implementation of the SDP specification, in particular, to handle the distributed denial of service attacks while also handling attacks like credential theft, server misconfigurations, and vulnerable code. This adoption is changing the current approach to security by:
    i. Changing the security strategy from compliance- to a risk-based culture
    ii. Expanding adoption and expansion of the CSA SDP Specification

c. What can or should be done now or within the next 1-2 years to better address the challenges;
With the advent of a reference implementation of the open source SDP, NIST has already started to include SDP in several of its new cloud security publications for adoption. Pilots and prototypes of SDP within critical infrastructure networks over the next few years will fuel the widespread adoption of a risk mitigation strategy that has proven to stop all network attacks. SDP will stop attacks like distributed denial of service and malicious code attacks, cross-domain insider threats like man-in-the-middle attacks and reduce the risk to a small set of insider attacks that organizations can now focus on securing. This strategy will allow:
    i. The move toward risk management and place the responsibility with the C-suite and business owners
    ii. The focus on risk mitigation on the high-risk applications rather than the entire enterprise

d. What should be done over the next decade to better address the challenges; and
The current trend to fund an IP-based network security strategy must be changed to accommodate a sound ‘connection-based’ security strategy. The result will put the onus of securing critical infrastructures on the business owners/leaders rather than the IT staff who are most often unaware of the business risks of their decisions.
    i. Adopting a risk mitigation strategy that is based on risk evaluations that can differentiate risk value and security posture and transfer the remainder through cyber insurance

e. Future challenges that may arise and recommended actions that individuals, organizations, and governments can take to best position themselves today to meet those challenges.
Adopting any paradigm that changes the status quo from network security to digital risk management requires commitment from executives and governments to take the lead. Education and guided conceptions need to occur here so that the following three changes occur throughout an organization.
    i. Culture change to a digital risk management strategy
    ii. Funding and Insurance provided at the right time to the right organization
    iii. Leadership that provides not only a vision but metrics and progress goals

B. Emerging technology trends and innovations;

a. The effect these technology trends and innovations will have on the digital economy, and the effect these technology trends and innovations will have on cybersecurity.

   Moving to a strategy to quantify, reduce and control digital risk allows organizations to make measurable decisions to overcome weaknesses in critical infrastructure and the impacts they create in the economy. A 'connection-based' economy is already emerging, and technologies are being adopted at a rapid pace to enable this economy, e.g., Google, Facebook, etc. Securing these connections should be paramount in guiding innovations.

   Cyber security as we know it today will be obsolete with the adoption of secure architectures such as the one SDP affords.

b. Economic and other incentives for enhancing cyber security.

   The biggest advantage SDP has over current cyber security trends is that Cyber Insurance which today ONLY covers cyber breach response will morph into Digital Risk Insurance that will be inherently designed to cover critical infrastructure.

   i. By moving to a risk management culture, cyber insurance will be replaced with digital risk insurance and the impact of cyber exploitations will be minimized
   ii. Adoption of the CSA SDP specification will make cyber security solutions much less complicated or obsolete
   iii. Significant reduction of the cost of cyber security protection will ensue while at the same time addressing the shortfall in cyber security professionals required to address cyber events as we know them today

c. Government-private sector coordination and cooperation on cybersecurity.

   Work is already underway to evangelize the government and private sector coordination under the umbrella of the Digital Risk Management Institute. The framework provided by the Institute can be used to benchmark organizations using 'evaluations' instead of 'assessments' that provide deeper insight into the protection of critical infrastructure. Also, the Cloud Security Alliance has brought this conversation to the forefront by adopting it as a guideline for their membership.

   i. A joint perusal of the CSA SDP specification will enhance national security by making securing the elements of the critical infrastructure less complicated, less costly and more secure.
   ii. A joint perusal will lower the cost hurdle for the private sector to secure the critical infrastructure to minimize or eradicate the need to pass costly cyber security solutions on to the consumer

d. The role(s) of the government in enhancing cybersecurity for the private sector.

   Government will play a huge role in changing the current cyber security trend and re-focusing cyber dollars to be spent on actually securing critical infrastructure rather than focusing on assessments and mandates. The time to do this is now.

   i. Government can spearhead joint pilots to prove that the SDP can secure critical infrastructure in the various sectors. (https://www.dhs.gov/critical-infrastructure-sectors)
   ii. Grants for independent pilots that require outcome reporting and adoption based on successful outcomes (both cost and cyber security) will be paramount to the success of SDP

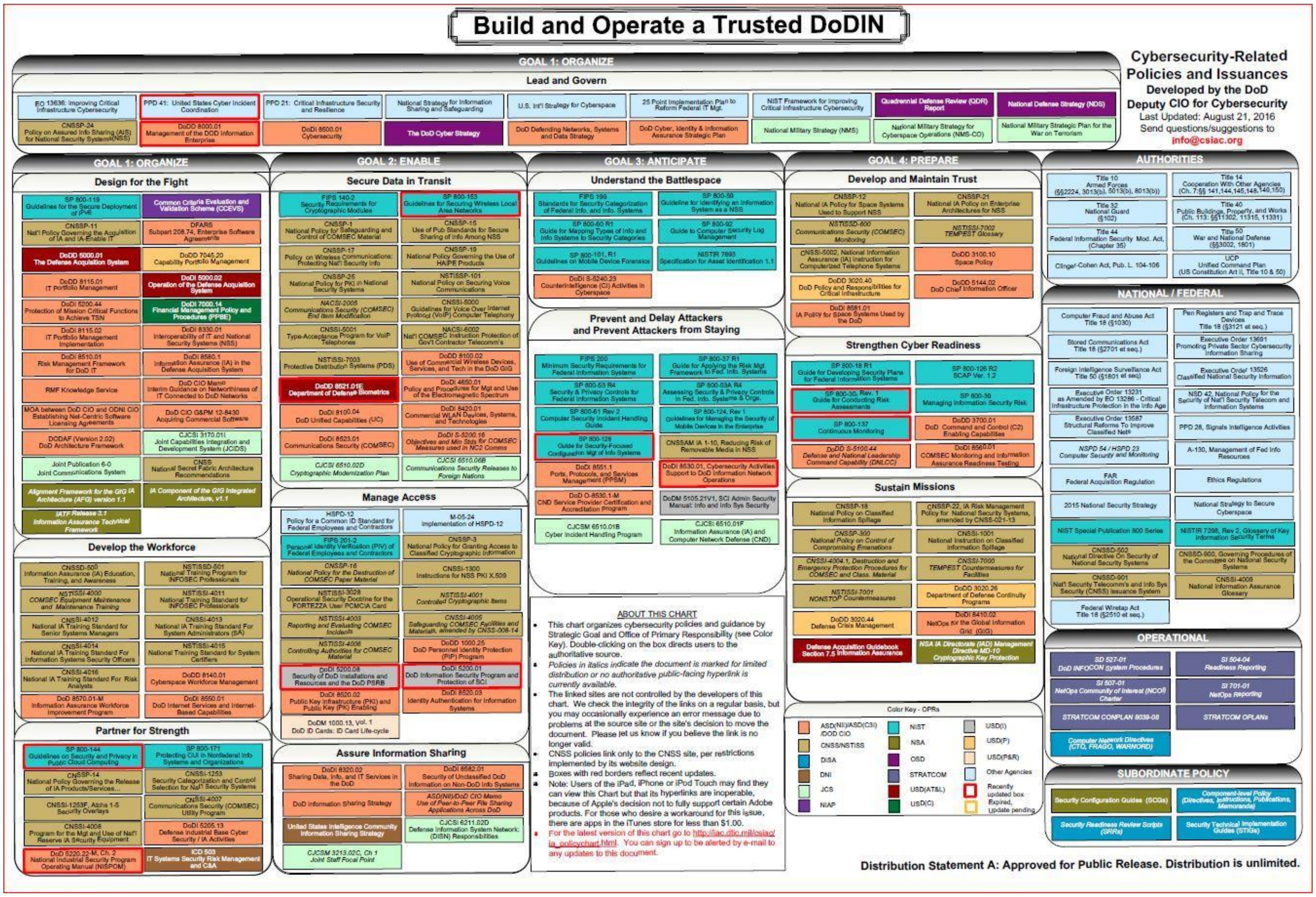
e. Performance measures for national-level cyber security policies; and related near-term and long-term goals.
Today's measurement goals for cyber security involves confidentiality, integrity and availability scores that are hard to measure and are subjective. Vulnerability scores, configuration management scores and the like only confound the problem of providing simple metrics. Performance measures in the form of KPRs for each critical infrastructure sector have already been studied and identified. Governments need to focus on these KPRs for each sector and require that industry step up to the plate to reduce the risk and enhance KPRs that are already defined. (https://www.dhs.gov/critical-infrastructure-sectors)

Also, for the SDP pilots, the following metrics will need to be studied and tied to the KPRs described above.

i. Level of Security / Hardening
ii. Cost Effectiveness

f. The complexity of cybersecurity terminology and potential approaches to resolve, including common lexicons.

Given that organizations need to focus on their mission, the complexity of implementing cyber security needs to be greatly reduced. The following chart says it all. It is next to impossible for organizations to cost-effectively provide the level of cyber security required while maintaining their mission.


Build and Operate a Trusted DoDIN
GOAL 1: ORGANIZE
Lead and Govern
Cybersecurity-Related Policies and Issuances Developed by the DoD Deputy CIO for Cybersecurity
Last Updated: August 21, 2016
Send questions/suggestions to info@csiac.org
GOAL 1: ORGANIZE
Design for the Fight
Develop the Workforce
Partner for Strength
GOAL 2: ENABLE
Secure Data in Transit
Manage Access
Assure Information Sharing
GOAL 3: ANTICIPATE
Understand the Battlespace
Prevent and Delay Attackers and Prevent Attackers from Staying
GOAL 4: PREPARE
Develop and Maintain Trust
Strengthen Cyber Readiness
Sustain Missions
AUTHORITIES
NATIONAL / FEDERAL
OPERATIONAL
SUBORDINATE POLICY
Color Key - OPRs
ASD(NII)/ASD(C3I)/DOD CIO
CNSS/NSTISS
DISA
DNI
JCS
NIAP
NIST
NSA
OSD
STRATCOM
USD(AT&L)
USD(C)
USD(I)
USD(P)
USD(P&R)
Other Agencies
Recently updated box
Expired, Update pending
ABOUT THIS CHART
This chart organizes cybersecurity policies and guidance by Strategic Goal and Office of Primary Responsibility (see Color Key). Double-clicking on the box directs users to the authoritative source.
Policies in italics indicate the document is marked for limited distribution or no authoritative public-facing hyperlink is currently available.
The linked sites are not controlled by the developers of this chart. We check the integrity of the links on a regular basis, but you may occasionally experience an error message due to problems at the source site or the site's decision to move the document. Please let us know if you believe the link is no longer valid.
CNSS policies link only to the CNSS site, per restrictions implemented by its website design.
Boxes with red borders reflect recent updates.
Note: Users of the iPad, iPhone or iPod Touch may find they can view this Chart but that its hyperlinks are inoperable, because of Apple's decision not to fully support certain Adobe products. For those who desire a workaround for this issue, there are apps in the iTunes store for less than $1.00.
For the latest version of this chart go to http://iac.dtic.mil/csiac/ia_policychart.html. You can sign up to be alerted by e-mail to any updates to this document.
Distribution Statement A: Approved for Public Release. Distribution is unlimited.

We are advocating reducing this terminology to 10 simple common terminologies that describe the power of leveraging SDP to stop all network-based attacks, to stop all cross-domain insider threats and to provide ample resources to protect oneself from the insider threat.

1) user authentication
2) user authorization
3) device authentication
4) device authorization
5) application / infrastructure binding
6) secure communications / encryption
7) secure configuration
8) key management
9) vulnerability management
10) behavior analysis of application / infrastructure