Written Testimony
U.S. House Committee on Homeland Security
Subcommittee on Cybersecurity and Infrastructure Security
"CDM, the Future of Federal Cybersecurity?"
Dan Carayiannis
RSA Security, RSA Archer Global Public Sector Director
January 17, 2018

Introduction

Chairman Ratcliffe, Ranking Member Richmond, and Members of the Committee, thank you for the opportunity to testify today on the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) program. I applaud the Committee's efforts to improve cybersecurity across the federal government and commend the Committee's initiative to better understand this mission critical program.

My name is Dan Carayiannis and I am the RSA Archer Global Public Sector Director for RSA Security, part of Dell Technologies. I have been part of the RSA Archer business unit for 10 years and I'm the RSA lead for the DHS CDM Dashboard. I also lead Archer's initiatives in the federal, state, local and international public sector. I have spent over 30 years in the information technology industry.

RSA has been a cyber industry leader for more than 30 years. The more than 14,000 global customers we serve represent many sectors of the economy. Our business helps enable those we work with to effectively detect, investigate, and respond to advanced attacks; confirm and manage identities; and ultimately reduce intellectual property theft, fraud, and cybercrime.

Today, I want to explain how RSA Archer is designed and deployed, how it helps DHS drive greater cybersecurity, and our CDM program recommendations.

About RSA Archer

RSA Archer is a commercial off-the-shelf technology platform that allows organizations to manage multiple domains of risk in a configurable, integrated software system. RSA Archer is the software solution the CDM program is using as a basis for both the agency and federal dashboards. Our platform and solutions support a range of needs to include a flexible data architecture, integration capabilities, reporting and dashboards, analytical functions as well as notification and workflow functionality. These capabilities provide users with the ability to interact, gather information and manage data beyond merely cataloging records. With RSA Archer, risk and compliance teams can better manage risks, escalate issues, streamline processes and make decisions based on the improved organization of data.

RSA Archer has been a technology solution provider in the Governance, Risk, and Compliance industry since 2000. The platform has approximately 1,400 deployments globally, including many of the Fortune 100 companies and government entities. RSA Archer is used in a variety of applications and methods, ranging from global, cross functional programs such as enterprise level risk management to single function or regional implementations to support defined use cases.

Risk and security management in today's world must be approached as an integrated business solution for a complex business challenge. The RSA Archer Suite includes multi-disciplinary risk management solutions and use cases that address the most critical domains of business risk. RSA Archer solutions incorporate industry standards to quickly implement the processes to achieve the visibility business and technology leaders need. Our use cases have adopted best-practice standards derived from our extensive customer base and industry standards including NIST 800-53, NIST 800-30, NIST CSF, FISMA, ISO31000, ISO27000, COSO, ISO22301 and more. RSA Archer solutions are also designed with a maturity-driven approach that enables organizations to implement risk management processes over time. Our use case model allows customers to target the organization's most pressing needs by mixing and matching use cases as the business requires.

All RSA Archer solutions are implemented on the RSA Archer platform, allowing an organization to build a consolidated technological approach to managing security, risk and compliance processes. We understand risk, security and compliance programs require a flexible, sustainable approach and our technology is designed to be highly configurable and customizable. The RSA Archer platform enables organizations to modify RSA Archer use cases to meet their unique requirements with functionality such as configurable workflows, risk calculations, standard and ad hoc dashboard and reports and flexible technology agnostic data ingest capabilities. Customers are able to tailor applications to meet their business requirements without the need for extensive coding or development skills all of which is of significant benefit to the DHS CDM program. To meet more advanced needs, customers can leverage RSA Archer APIs and integrate external products to meet unique requirements.

RSA Archer features the following key capabilities:

- An integrated reporting engine and does not require external reporting tools;
- Persona-driven reports and dashboards are built into the solutions, along with the ability to create ad hoc reports and dashboards to meet users' needs;
- User interface designed to satisfy both frequent users (risk/compliance/security teams) and infrequent users (business users/first line of defense);
- Integration capabilities that allow organizations to consolidate data from external systems and range from data import to scheduled data feeds to an API;
- Data ingest capabilities that allow for integrations with external information sources without major code/development efforts to quickly consolidate and map external data to RSA Archer applications;
- Flexible risk scoring functionality as well as robust workflow and notification capabilities enable customers to automate business process.

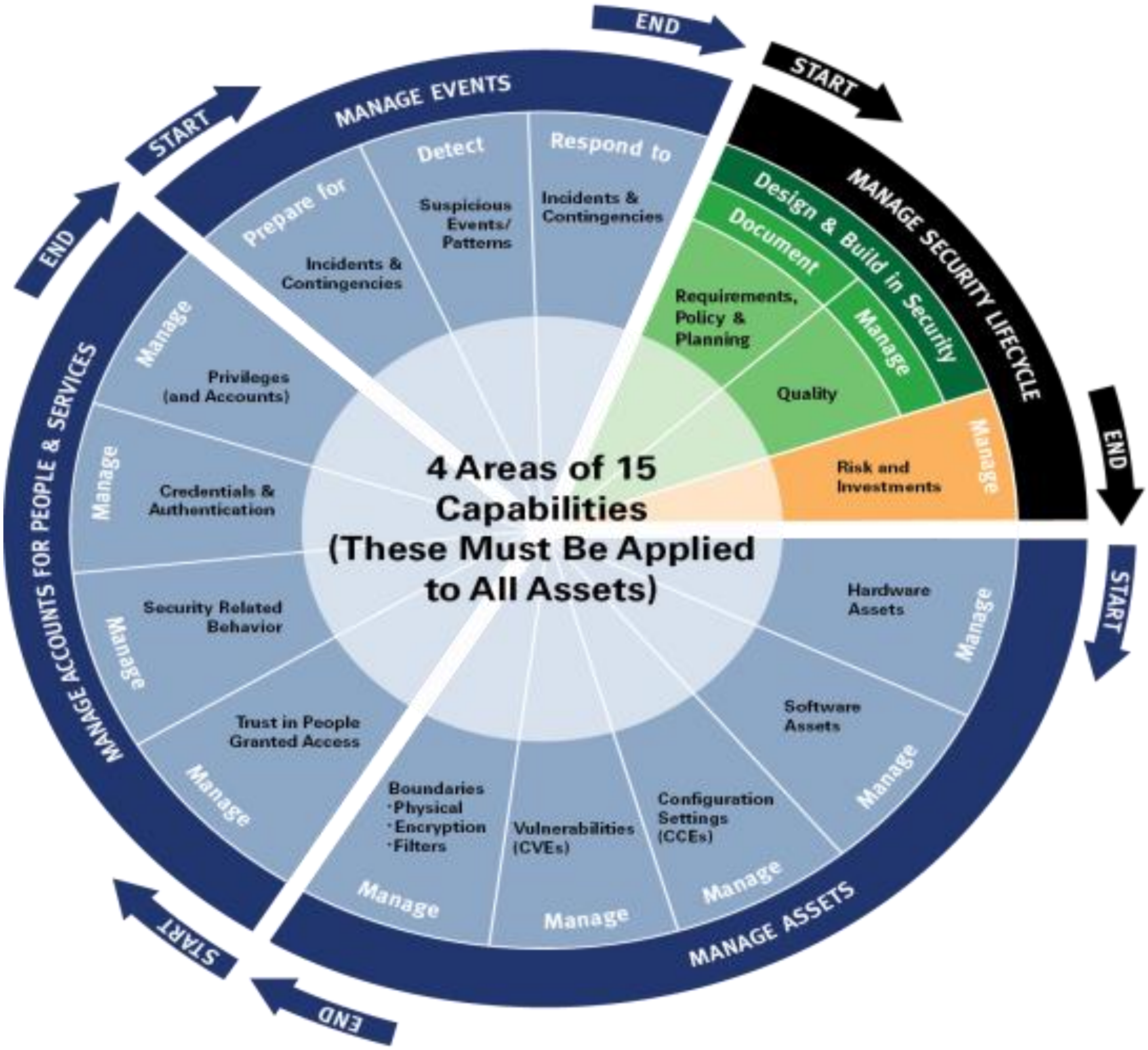
RSA Archer and CDM

The federal government is challenged with a broad range of continuous monitoring security maturity levels and efforts across a wide range of agencies. To address these challenges, CDM provides a framework that enables consistent and automated compliance monitoring and reporting, helps agencies understand risks and vulnerabilities that could impact the security and operation of their enterprise, and does so in a consolidated and accelerated timeframe.

RSA Archer provides the base software solution for CDM that is commercial off-the-shelf technology that's flexible, browser-based, scalable, easily deployed, and can be fully integrated within a comprehensive dashboard architecture to meet DHS' current and future dashboard requirements. The RSA Archer Continuous Monitoring software solution was built to meet the needs of federal agencies as well as commercial organizations by providing mission critical capabilities essential to the Continuous Monitoring program. In the case of CDM, the software is being configured and customized to support program requirements by MTV, the dashboard prime contractor under DHS's direction. These essentials are:

- Enabling near real time visibility into the security posture of targeted devices across the enterprise;
- Managing with a risk-based approach by prioritizing security risk data and focusing on "worst first";
- Maintaining a common operational cyber landscape with aggregation and correlation of data to stay current with latest requirements;
- Having real time alerting capabilities, and advanced reporting and dashboards at multiple levels of the organization in order to help protect infrastructure across network endpoint such as laptops, desktops computers and servers;
- Protecting sensitive information such as security configurations and vulnerability information while providing access to the proper individuals to mitigate risks;
- Tracking and reporting compliance across vulnerabilities, configurations, assets and applications; and
- Leveraging and maximizing existing and new agency infrastructure CDM tools.

The CDM project is segmented into multiple phases and functional areas as the DHS diagram below illustrates.



END
START
MANAGE EVENTS
Prepare for
Incidents & Contingencies
Detect
Suspicious Events/ Patterns
Respond to
Incidents & Contingencies
MANAGE SECURITY LIFECYCLE
Design & Build in Security
Document
Requirements, Policy & Planning
Manage
Quality
Manage
Risk and Investments
END
START
Hardware Assets
Manage
Software Assets
Manage
Configuration Settings (CCEs)
Manage
Vulnerabilities (CVEs)
Manage
Boundaries
·Physical
·Encryption
·Filters
Manage
MANAGE ASSETS
END
START
MANAGE ACCOUNTS FOR PEOPLE & SERVICES
Manage
Privileges (and Accounts)
Manage
Credentials & Authentication
Security Related Behavior
Manage
Trust in People Granted Access
Manage
END
START
4 Areas of 15 Capabilities (These Must Be Applied to All Assets)

Last Updated 12-Nov-2013

RSA Archer can support the functional areas as outlined by the scope of CDM. The following are examples of how RSA Archer is being used to support the phase 1 CDM functional area:

- **Functional Area - Hardware Asset Manager** - RSA Archer helps to manage a repository of hardware information assets as a result of its integration with the chosen hardware asset management tool. We are designed to help agencies determine asset classification ratings and required retention periods, determine asset risk, associate the assets with responsible individuals, locations, organizational units, processes they support, facilities where they are housed, and associated with applications they support. RSA Archer can leverage its notification and workflow functionality to support remediation efforts associated with hardware assets and can represent this information in reports, dashboards and web forms and permit access permissions down to the field level so that multiple levels and views are available to the appropriate organization and personnel for action. In addition, RSA Archer enables agencies to perform online assessments to support organization/agency wide data calls to determine classification ratings and required retention periods.

- **Functional Area– Software Asset Manager** - RSA Archer helps to manage a repository of software information assets as a result of its integration with your chosen software asset management tool. RSA Archer is designed to help agencies determine asset classification ratings and required retention periods, determine asset risk, associate the assets with responsible individuals, locations, organizational units, processes they support, facilities where they are housed, and associated with applications they support. RSA Archer can leverage its notification and workflow functionality to support remediation efforts associated with software assets and can represent this information in reports, dashboards and web forms and permit access permissions down to the field level so that multiple levels and views are available to the appropriate organization and personnel for action. In addition, RSA Archer enables agencies to perform online assessments to support organization/agency wide data calls to determine classification ratings and required retention periods.
- **Functional Area – Configuration Management** - RSA Archer consolidates data, helps determine asset, application and system risk, and associates configurations with controls, responsible individuals, locations, organizational units, processes they support, and facilities where they are housed. RSA Archer can leverage its notification and workflow functionality to support remediation efforts associated with configuration issues and can represent this information in reports or dashboards. RSA Archer provides an approach for documenting, identifying, managing, and reporting on configuration data at every level of the organization. RSA Archer allows agencies to consolidate controls across multiple regulatory and business requirements into one integrated framework.
- **Functional Area – Vulnerability Management -** RSA Archer consolidates threat data and reports on threat remediation activities and enables a consistent, repeatable threat management process. RSA Archer consolidates vulnerability, malicious code, and patch information from security intelligence providers, and captures vulnerability results from scan technologies into one threat-management system. RSA Archer then cross references this information with applications, assets, individuals and organizational units. RSA Archer leverages its notification and workflow functionality to support remediation efforts associated with vulnerabilities and can represent this information in reports, dashboards and web forms and permit access permissions down to the field level so that multiple levels and views are available to the appropriate organization and personnel for action.

In summary, RSA Archer is critical in helping DHS realize its goal of comprehensive CDM across the .gov landscape. This includes a hierarchical deployment of agency level dashboards rolling up summary results to the federal dashboard. RSA Archer's role is to aggregate summary data collected from various technologies and data stores, calculate and score risk, notify users of changing data, and enable workflow business processes. This aligns specifically with the concepts of RSA Archer as a system of engagement (gathering data and enabling processes) and system of insight (providing aggregated data for decision support).

Additionally, RSA Archer is helping DHS CDM address the many different personas interacting with the 'systems of engagement' and 'system of insight.' A simple way to think of this is to use the concepts of 1st, 2nd and 3rd Lines of Defense ("LoD"). This concept, referenced in operational risk management strategies, provides a straightforward method to stratify the risk management program and using Archer is being applied by DHS.

In terms of the CDM project, RSA Archer takes the rollup of data from 1st LoD (sensors, endpoints, etc. via a variety of technologies) to inform and drive mitigation activities at the 2nd LoD at the individual agency level dashboards and facilitating oversight and visibility to the 3rd LoD at the DHS Federal Dashboard level.

CDM Implementation and Recommendations

RSA is committed to CDM as its commercial software manufacturer and technology partner. We have actively worked with the DHS CDM Project Management Office ("DHS") as the "customer," as well as with the dashboard and prime contractors. We have ensured that our leadership is engaged with project and progress updates, have provided flexible licensing arrangements, and continue to evolve our technology strategy to meet CDM requirements today and anticipate future needs. We meet regularly with key stakeholders within DHS and prime contractors to ensure our technology is aligned to DHS's requirements.

To this end, we have expanded several of our development plans to ensure DHS benefits from the CDM program improvements. DHS, CDM and Archer are pushing the boundaries on how a large enterprise should think about, manage and respond to today's security threats as well as prepare for tomorrow's unknowns. This project not only benefits our nation's security but provides significant private sector security benefits as well.

To date, we have undertaken and released several product enhancements aligned with DHS's requirements. For example, in the 6.3 version of our platform, released in October 2017, several improvements and architectural changes were made based on feedback from DHS and its contractors to accelerate data ingest processes. We are also working on additional changes to ensure RSA Archer meets its design goal of flexibility and also enhanced performance for data management and calculations which will help DHS make risk based decisions in near real-time.

We are supporting the CDM program through the dashboard contractor MTV and also through the various prime contractors. This support is being provided through our Technical Support, Services and Engineering organizations. While we are the software manufacturer, we fully recognize the role and functional elements of the agency level as well as the federal dashboard and continue to fine tune our base software solution and platform to accommodate defined and anticipated requirements.

As a result of our experience and involvement with DHS in the CDM program, we propose the following recommendations:

First, we strongly encourage DHS to maintain ongoing control of the dashboard. We see the CDM dashboard as both a strategic executive risk management visualization tool as well as an agency operational tool. Standardization and consistency across the government is critical to program success and having a standardized risk management approach with one organization, DHS, responsible for managing cyber security risk across the civilian government marketspace is a primary reason we believe the program is succeeding. DHS may not be able to respond in a timely fashion without a centralized management approach or if it is being constrained by a distributed agency funding model. Once fully deployed, we believe this highly controlled approach will render more consistent and accurate metrics across the government, better cyber risk based decisions, where necessary faster remediation and encourage standardization and a common consistent measurement and expression of risk across the federal government. Regardless of the deployed tools and data stores used, centralized management and standardized risk scoring methodology provides a true "apples to apples" comparison from agency level dashboards to the federal level dashboard, giving the government confidence in consistent measurement and representation of risk.

Second, we encourage DHS to continue facilitating a shared vision approach for program success. Continued dialog among DHS, RSA, and the dashboard and group prime contractors allows us to reflect on our base software architecture and plan for future software enhancements to benefit the program going forward. We also recommend DHS continue to allow RSA to participate in DHS and its dashboard prime contractor technical exchange meetings on a quarterly or semi-annual basis so we can stay current with anticipated requirements.

Third, we encourage an active, ongoing training program as part of the CDM initiative. The contractors who have invested in RSA Archer training have accelerated their learning curve on Archer and increased their deployment success. As DHS CDM dashboards are fully deployed across the federal civilian agencies, we believe its critical agency prime contractors have RSA Archer Administrators with the skills and experience necessary to maximize dashboard capabilities.

We also recommend DHS personnel participate in RSA Archer training to better understand the RSA Archer platform as it relates to the DHS CDM program and in the future. With the successful rollout of dashboards across all government agencies, we recommend agency personnel "user" training to maximize the value DHS and the government are getting out of its dashboard investment such as embedded training videos, on-line training and more.

Fourth, we recommend careful considerations be put in place during the dashboard re-compete process. We believe the follow-on dashboard prime contract holder should have the necessary RSA Archer skills and capabilities to accept dashboard responsibilities "mid-stream" and continue to manage, configure and customize the dashboard without issue. Given the learning curve we have seen the dashboard contractor go through to configure and customize RSA Archer to support DHS CDM dashboard requirements, ensuring technical personnel are fully trained and experienced is a prudent and necessary element of continued success.

Fifth, we urge the subcommittee to continue its strong support of the CDM program and ensure it has the necessary authorization and resources for full and expanded implementation. It is essential DHS has the necessary funding for the ongoing phases of CDM to build upon the current implementations and success.

Finally, we encourage CDM information be analyzed for benefits beyond the immediate CDM scope. One of the bi-product benefits of the DHS CDM program is that agencies can leverage CDM aggregated data to support other "out of scope" agency requirements. For example, agencies can enhance their assessment and authorization and continuity of operations processes by leveraging critical data elements CDM has captured. We believe this saves the government not only time but also funding.

Conclusion

In closing, we believe the CDM program is having a very positive impact on how governments as well as commercial organizations think about managing cyber risk. In today's world, cyber threats are real, coming from multiple vectors, and constantly changing. RSA believes the CDM program is well positioned to help the federal government better understand and react to these cyber threats.

Thank you Chairman Ratcliffe and Ranking Member Richmond and all members of the subcommittee for your dedication to addressing cybersecurity and to the CDM program. I thank you for the opportunity to be here today and I look forward to working with you and your colleagues in Congress as cybersecurity remains at the forefront of so many policy decisions we face. I'd be happy to answer any questions the subcommittee may have.