CRISP RSS
connection

• A new look for Chantilly
• Spotlight on ASD team
• PIV, e-QIP, and CFE

IN THIS ISSUE
• Why CRISP RSS matters
• Meet our new Managers

The Program Newsletter for CRISP RSS Team Members

SECOND QUARTER 2016

CRISP RSS LEADING THE WAY

It's hard to believe that a year ago this month, Continuous Readiness in Information Security Program (CRISP) Remediation Services Support (RSS) had just launched.

Today—one year later—we are at more than 700 people strong, supporting almost 280 U.S. Department of Veteran Affairs (VA) facilities with 12 functional teams.

And we're showing significant and measurable results in initiatives that we've worked on, while we continue to launch new endeavors.

Two-Factor Authentication (2FA)

In August 2015, the Two-Factor Authentication (2FA) team launched with the mission of implementing two-factor authentication for remote users throughout the agency to better protect VA data.

In seven months, our team helped VA conclude enforcement for more than 102,000 remote users and successfully enroll more than 24,500 users in MobilePASS®, which VA used to achieve 100% Citrix Access Gateway (CAG) One Time Password (OTP) enforcement. The 2FA team has also created a user time zone-sensitive ticket system, which has serviced more than 7,000 user tickets to date.

Securing Network Access for Medical Devices

A VA priority is securing patient data that resides on medical devices. To help VA meet this priority, Medical Device Protection Program (MDPP) is nearing completion of reviewing and updating Access Control Lists (ACLs) for medical devices residing on VA networks. So far, our team has reviewed over 4,000 ACL rule sets which in turn are being updated in VA routers that manage access for these devices.

Continued on page 2

Continued from page 1

Comprehensive pre-OIG Support

In March, the CRISP RSS program began assisting VA facilities in preparing for the annual Office of Inspector General (OIG) audits. There are 100+ CRISP RSS resources from 11 project teams directly assisting the facilities' efforts to prepare for the inspection.

CRISP RSS assisted VA in preparation for these audits at a handful of VA sites following the program launch last year. However, this year, the support is much more comprehensive and pro-active – members of the CRISP RSS team have visited 18 of the slated 24 locations, reviewing information systems, processes, and required documentation items prior to the OIG audit in a focused effort to find, analyze, and remediate vulnerabilities. Examples of support include helping sites remove prohibited software from desktops, securing networked medical devices, updating Incident Response Plans (IRPs), patching printers, and reviewing data backup procedures. Ongoing review and monitoring continues remotely after the pre-site prep activities conclude.

Backup and Data Encryption

With the start of Option Year 1, expansion of services in key areas has begun. One of the new teams is Backup and Data Encryption (BDE). BDE's goal is to help VA ensure that Veterans' Protected Health Information/Personally Identifiable Information (PHI/PII) are properly and securely backed up. Currently the BDE team is surveying VA facilities to understand how data is being backed up. Using this information, BDE will help VA implement plans to strengthen current backup practices at the regional and local levels.

By working in partnership with the customer, the BDE team has created a communications link to gain further insight into VA's vision, and continues to deliver documentation with a solid plan for how to best accomplish the goal of backing up and encrypting data for an enterprise solution.

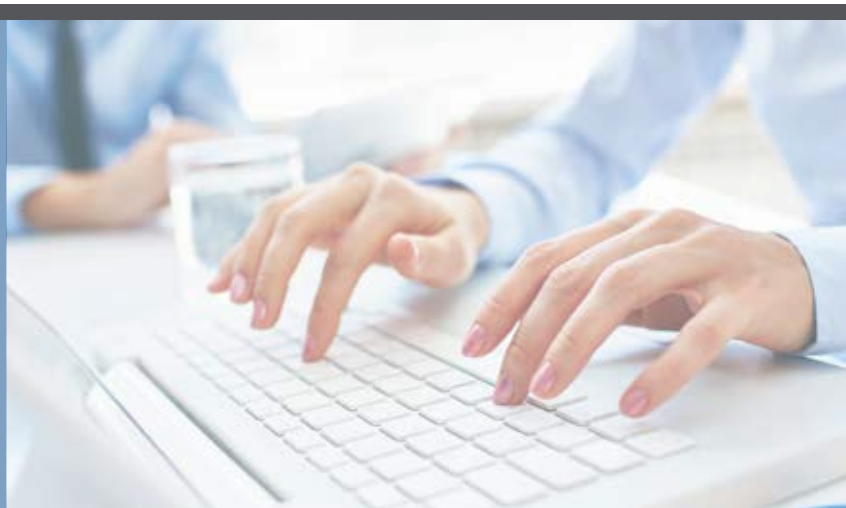
Program-wide View

Of course, we have many more efforts underway in addition to the projects I described above. From the installation of routers that encrypt network traffic, to removal of over 13,000 instances of prohibited software, you are the ones helping drive improvements in VA systems. The CRISP RSS team is one of which I am proud—and one our customer can rely upon for measurable results. Stay focused, understand the opportunity for real change that we have, and keep up the great work you do every day.

Doug Shorter

We'd love to hear from you!

Please submit newsletter suggestions, comments and story ideas by clicking on the following link in the CRISP RSS SharePoint site: *https://rss.asmr.com/CRISP_RSS/Lists/Newsletter%20Suggestions/overview.aspx*.



Congratulations!

The **Platforms Team** was recognized by Ray Walsh, Chief, Platforms & Operating Systems Division, Region 4 Core Systems for their outstanding performance in March 2016. Congratulations to these Platforms Team members: **Jeffrey Condon**, Information Science; **Patrick Ferraro**, MKS2; **Michael Barbalace**, **Danny Hynes**, **Susan Kosier**, and **Christopher Medeiros**, ASM Research; **Jon Mercure**, QuarterLine Consulting; **Lamarr Turner**, and **Joseph Villapaz**, xScion Solutions.

Ariel Montano Cardenas earned a Masters degree in Cybersecurity from Marymount University in Arlington, VA.

Erick Lavelle earned Certified Information Systems Security Professional (CISSP) certification in January 2016.

Congratulations to **Ryan Summers** for all of his successes as Team Lead of the Medical Device Protection Program (MDPP). We appreciate all of his hard work and leadership and wish him continued success with his other AFS projects.

Sharing is caring—let everyone in on your big news and CRISP RSS accomplishments!
Click on this link to submit your notices: *https://rss.asmr.com/CRISP_RSS/Lists/Newsletter%20Suggestions/overview.aspx*

GOT NEWS? **BRING IT ON!**

Calling all CRISP RSS employees! ***Connection*** is *your* newsletter. Its purpose is not only to inform you about what's happening in the CRISP RSS program but also give you a platform on which to shout out some good and/or fun news. So if you've got anything cool you'd like to share, send it here and we'll make you famous.

What kind of items are we looking for, you ask? Here's a list:

- Birthdays
- Promotions/new job responsibilities
- Awards
- Fun vacations
- New babies
- Weddings
- New degrees or certificates
- Graduations
- Your lottery winnings (not really, but if you'd like to share, please do)
- Engagements

CRISP RSS
CHANTILLY 2.0

"Where are you sitting now?" If you work at the CRISP RSS Chantilly campus, this answer has changed several times over the past five months. For many people on the project, it's par for the course; a majority of the teams are made up of either ex-military or military families, so relocating is in their lifeblood.

The exciting news is the suites have been updated, and the temporary seating situation has been replaced with sunny views and open floor plans.

Staying Agile

Upon entering suites 100 and 120 at 14850 Conference Center Drive in Chantilly, you'll be impressed by the amount of available natural light in the workspace. Team members have been seated together for a more collaborative environment, which enables teams to stay agile in their organic work effort. Stations have been equipped with updated monitors, docking stations, and desk phones–enabling quick expansion of teams as needed or accommodating visitors to the campus. A current floor plan of CRISP RSS team locations can be found here: *https://rss.asmr.com/CRISP_RSS/PM%20Documents/CRISP%20RSS%20Team%20Seating%20Chantilly%20516.pdf?Web=1*

Suite 150 in 14840 Conference Center Drive has also been revamped and boasts an open, bright workspace with small meeting tables scattered throughout the various team areas. These spaces are perfect for impromptu gatherings as well as daily "stand-up" meetings. As with the suites in building 14850, team members are seated together in a table-style work environment to facilitate collaboration as the CRISP RSS program moves forward with Option Year 1 efforts.

Let's Get Together

There are six conference rooms as well as several "huddle" locations for employees to use at the Chantilly campus. The conference rooms are easily reserved via Outlook, so please be kind to your fellow CRISP RSS team members by booking your room in advance. Rooms are designated by their names in each suite. ♦

NEED A MEETING ROOM?

All Chantilly campus conference rooms are reserved by room name via Outlook:

Harrison / Suite 100 *ConfChantillyHarrison@asmr.com*
Hugo / Suite 150 *ConfChantillyHugo@asmr.com*
Monroe / Suite 120 *ConfChantillyMonroe@asmr.com*
Poe / Suite 150 *ConfChantillyPoe@asmr.com*
Taylor / Suite 120 *ConfChantillyTaylor@asmr.com*
Tyler / Suite 100 *ConfChantillyTyler@asmr.com*

PLANS OF ACTION

This quarter, CRISP RSS is engaged in numerous Plans of Action, including:

FY15 26 System and Network Monitoring

Identify external network interconnections. Improve processes for monitoring VA networks and systems. Create exchanges for unauthorized activity
VA POA POC: John Killian
CRISP RSS POC: Sam Giles

FY15 11 Field Security Support

Eliminate the number of elevated privileges granted to system users with unauthorized access rights
VA POA POC: Randy Ledsome
CRISP RSS POC: Duane Truax

FY15 18 / 19 Medical Device Protection Program

Implement improved network access controls to segregate medical devices and non-OI&T networks from general and mission-critical systems under common control
VA POA POC: Lynette Sherrill
CRISP RSS POC: Ryan Summers

FY15 13 Implementation of Two-Factor Authentication

Implement 2FA for all local and remote access throughout VA
VA POA POC: Terry Luedtke
CRISP RSS POC: David Jones

FY15 28 / 29 Unauthorized Software Remediation

Develop comprehensive list of approved and unapproved software and implement monitoring processes and prevent unauthorized software
VA POA POC:
Jacqueline Meadows-Stokes
CRISP RSS POC:
Rosemarie Jernigan

FY15 12 Enable System Audit Logs

Implement SIEM-based log monitoring to generate system security alerts and detect security violations
VA POA POC: Tery Brownelle
CRISP RSS POC: Jon Mervine

FY15 8 / 9 Accreditation Documentation Remediation

Develop security plans and improvement processes for reviewing and updating key security to address ~9,500 POA&Ms affecting VA facilities and systems
VA POA POC: Rob Disko
CRISP RSS POC:
Kimberly Williams

FY15 15 / 16 Patch and Vulnerability Management

Implement P&VM program to improve processes and automated mechanism to remediate VA security deficiencies
VA POA POC: Chris Helsel
CRISP RSS POCs:
Aubrey Campbell, Erik Lavelle and Sami Mousa

FY15 5 POA&M Artifacts

Ensure sufficient supporting documentation is captured in the central Governance Risk and Compliance tool to justify closure of POA&M
VA POA POC: Rob Disko
CRISP RSS POC: Duane Truax

FY15 17 Configuration Baseline Scanning

Maintain complete and accurate baseline configurations to be in compliance with VA security standards
VA POA POC: Chris Helsel
CRISP RSS POC: Aubrey Campbell

FY15 22 Backup Encryption Data

Develop and implement a process for ensuring the encryption of backup data prior to transferring the data offsite for storage
VA POA POC: Dewayne Porter
CRISP RSS POC: Yaa Ansah Pobi

FY15 10 Password Policy Enforcement

Enforce VA Password policies and standards on all operating systems, databases, applications and network devices
VA POA POC: Chris Helsel
CRISP RSS POC: Aubrey Campbell and Sami Mousa

FY15 21 Info. System Contingency Plans

Implement processes to ensure information system contingency plans are updated with the required information
VA POA POC: John Killian
CRISP RSS POC:
Kimberly Williams

2006 04 Background Investigations

Ensure appropriate levels of background investigations are completed for all personnel in a timely manner
VA POA POC: Trish Moore
CRISP RSS POC: Troy Williams

UP NEXT FOR CRISP RSS

- The third **All Hands meeting** was held May 12, 2016–the video is available on CRISP eLearn at *https://crisplearning.asmr.com/course/view.php?id=21*. Look for the next **All Hands meeting** late summer.
- **Sprint Reviews** are held monthly and showcase valuable program milestones to VA leadership. You can review past presentations by following this link: *https://rss.asmr.com/CRISP_RSS/Sprint%20Reviews/Forms/AllItems.aspx*.

YOU, YOUR PIV, E-QIP, AND CFE

You've likely noticed that the CRISP RSS program uses a number of acronyms including three which impact you directly: PIV, e-QIP, and CFE. What are these things and why do you need them?

Personal Identity Verification (PIV)

You'll need a PIV card to gain access to VA information systems. A PIV card is a U.S. federal smart card containing your personal data—who you are, your biometric data (which includes your fingerprints), where you work, your occupation, and other critical information. To log in to a particular VA site, insert your PIV card into your computer's card reader, and if your credentials prove valid, you are granted access to the site. Why all of this background investigating, you ask? Because it's important to ensure that the sensitive information about our Veterans is protected. People who are granted access to VA information networks must be individuals who pass a background check.

To get a PIV card, you must be sponsored by the Contracting Office Representative (COR), who will email you an application. You will also need a Transmittal Notice, which you receive after your e-QIP (see below) has been adjudicated. When you receive the Transmittal Notice, notify a CRISP RSS Information Security Officer (either Donna Chandler or Leesa Morgan).

What brought about the PIV card?

In August 2004, President George W. Bush issued Homeland Security Presidential Directive 12 (HSPD-12), which mandated new standards for secure and reliable identification for all federal employees and contractors. The encrypted data in a PIV card helps strengthen the security of not only your personal information, but also that of Veterans as well, since access to secured VA areas depends on your PIV card.

Electronic Questionnaires for Investigations Processing (e-QIP)

Before you can apply for a PIV card, you must complete e-QIP. This electronic package is emailed to you (when it's sent can vary) and involves filling out a number of questionnaires about yourself so that the government can investigate your background. The questions will require information such as where you grew up, where you went to school, every place you've ever lived, every phone number you've ever had, people who know you, any arrests or convictions you may have had; all that and other personal information goes into your e-QIP. You'll want to gather all of this personal data now, so you have it available before you plunge into e-QIP.

Contractor-Furnished Equipment (CFE)

Chances are you'll be required by contract to use equipment provided by ASM and software imaged by VA, issued specifically to you. A CFE laptop not only enables you to access VA networks and information systems, but also helps keep them safe and secure.

The Process

The cornerstone of all this is e-QIP; without it, you don't get your PIV card or CFE. Here's the process:

- Fill out and submit your e-QIP.
- After VA adjudicates your e-QIP, you receive a Transmittal Notice, which enables you to get your PIV card. You'll then go to your local VA facility to get fingerprinted. It is important to notify Donna Chandler when you receive this notification.
- You will be issued a VA account.
- You'll receive notice that your PIV card can be picked up from the VA facility that recorded your fingerprints.
- Finally, if you have a VA account and a PIV card, you may be issued a CFE.

And here's a big DON'T: Do not contact VA unless you're instructed to do so. Go to your team's Point of Contact (POC) for any VA access, PIV card, or e-QIP issues.

So there you have it: PIV, e-QIP, CFE. They might seem like alphabet soup, but they are essential in the service we provide to our nations' Veterans. ♦

What do you want to know about CRISP RSS? Please submit any questions or suggestions for this column by clicking on the following link in the CRISP RSS SharePoint site: *https://rss.asmr.com/CRISP_RSS/Lists/Newsletter%20Suggestions/overview.aspx*. These will be addressed in subsequent issues of the newsletter.

Getting to Know...ASD Team

The CRISP RSS Architecture, Strategy and Design (ASD) team supports the VA in its efforts to remediate unauthorized software installed on its network. Rose Jernigan, Team Lead for ASD, is heading up this initiative from the Charleston, South Carolina CRISP RSS office.

Unauthorized software includes unapproved and unmanaged software as well as prohibited software. “Unapproved” is software that has not been approved for general use. “Prohibited” is software that is not currently permitted to be used under any circumstances. “Unmanaged” is software that has yet to be evaluated.

The remediation process includes the creation of National Service Desk (NSD) tickets, drafting of National Action Items, and coordination with VA and CRISP RSS onsite staff. Through these efforts, the ASD team helps mitigate security vulnerabilities on the VA network.

Unapproved or Prohibited?

Members of the ASD team support the Technology Reference Model (TRM) authoring process by providing analysis and classification recommendations. In analyzing questionable software applications, ASD team members often contact the software vendor for details about the software application to determine how to classify the title (approved, approved with constraints, unapproved, divest, or prohibited).

The team then uses the System Center Configuration Manager (SCCM) to generate two reports—one for unapproved software, one for prohibited. ASD utilizes SCCM to provide information regarding patch management and software distribution, including what regions, sites and systems have the unapproved/prohibited software titles and/or the versions installed. ASD team members assist in keeping SCCM unapproved and prohibited software reports in sync with TRM, which updates the prohibited and unapproved lists monthly.

Goal: Zero Prohibited Software

Although the OIG has noted that VA has made progress in developing policies and procedures to strengthen its information security and meet Federal Information Security Management Act (FISMA) requirements, more work needs to be done. The CRISP RSS program is here to provide that help, and ASD is making dramatic accomplishments.

“We’ve achieved more than 90% reduction in prohibited software since June 2015,” notes Jernigan, a 25-year IT veteran who has spent the past seven years in information security. ♦

USING SharePoint FOR REQUESTS

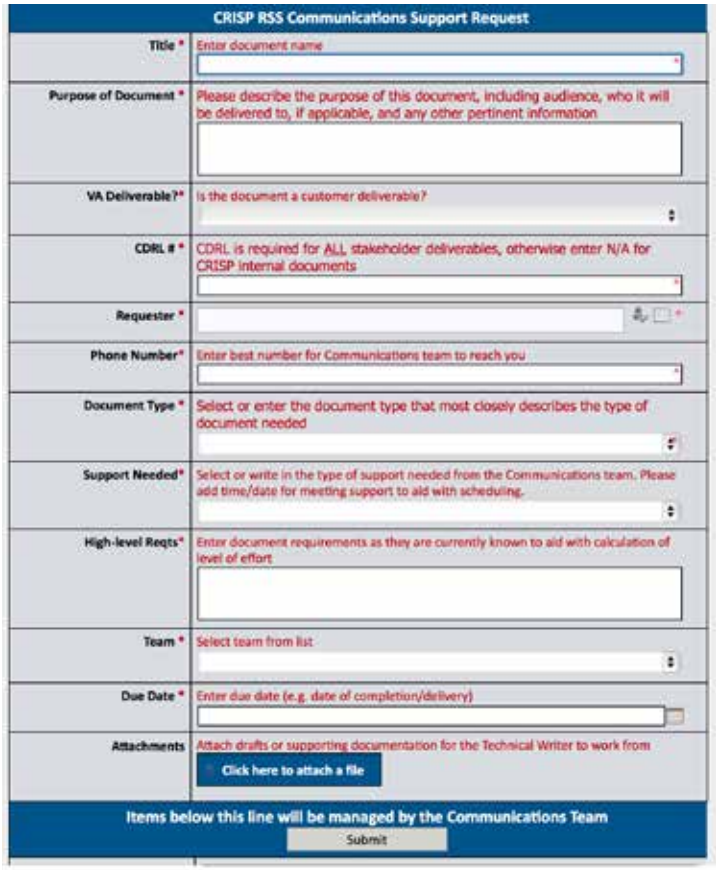
CRISP RSS team leaders, take note: If you want to produce any documents or presentations for your team or customer, you must go through the CRISP RSS Communications Team.

To do that, you fill out a Communications Request Form. To access that form, log on to the CRISP RSS SharePoint site, *https://rss.asmr.com/CRISP_RSS/default.aspx*.

1. Click the CRISP RSS Communications tab in the top navigation area, *https://rss.asmr.com/CRISP_RSS/Comms/default.aspx*.

2. Under "Lists," click "Communications Support Request." This will take you to the Communications Support Request Log page. Click on either "New Task" or the "+" sign next to it. The CRISP RSS Communications Support Request Form will appear, similar to the photo on the right.

3. Fill out the fields (use the drop-down arrows where applicable), scroll down to the "Submit" button, and click it.



That's it. You're done. The CRISP RSS Communications team leader will assign your request to a team member. When work on your request is completed you'll receive an email containing a link to your document or presentation. ♦

What's your CDRL number?

The Contract Data Requirements List (CDRL) Number is an identifier of an authorized data requirement for a specific procurement that forms a part of a government contract—think of it as a document's ZIP® code. Each document that is delivered to VA is required to have one, and like ZIP codes, several documents in the same class and category can be assigned the same CDRL number.

On April 28, 2016, CRISP RSS entered Option Year 1 (OY1) from the Base Year contract. This transition is also reflected in the CDRL numbers for many of the deliverables, but not all; several sections of the CRISP RSS documentation will continue in Base Year mode until September 2016.

A list of the current CDRL numbers can be found on the CRISP RSS SharePoint site, *https://rss.asmr.com/CRISP_RSS/PM Documents/CDRL Master List.xlsx*.

Unsure of your document's CDRL number? Check with your team lead for guidance. ♦

Welcoming new Leadership Team Members

Ian Fogarty

Deputy Program Manager

Wenceslao Angulo

Region 4 Manager

Michael Armstrong

Region 1 Manager

Maureen Brown

Project Manager, MDPP

Sami Mousa

Project Manager, NSOC

Yaa Ansah Pobi

Project Manager, Backup and Data Encryption

VA SECURITY THREATS: WHY CRISP RSS MATTERS

There is never any rest in the effort to protect VA data. The bad guys are hacking away, launching malware attacks and initiating other network threats like there's no tomorrow.

How prolific are VA security threats? In April 2015, VA detected more than 956 million attempted malware attacks, according to GCN, a Vienna, Va.-based publication providing technology assessments, recommendations, and case studies to public-sector IT managers. In April 2015, nearly 740 veterans had their personal health data compromised because of security vulnerabilities, GCN noted.

Two years ago, a security breach endangered the personal information of some 7,000 Veterans who had participated in a home telehealth program. In 2013, the OIG found 6,000 cybersecurity vulnerabilities in VA's network.

VA's staff of about 590 security professionals are busy safeguarding 750,000 connected network devices and daily monitoring 4.5 million emails and 55,000 new malware variants.

Protecting the health and personal data of our Veterans is a tremendous effort. That's why the CRISP RSS program is here. Needless to say, CRISP RSS security professionals are proudly helping VA in this good and crucial fight. ♦