Sentry-SECURE in the Field – A Summary of the Beta Test

E. Gonzalez
Pacific Northwest National Laboratory

B. Avery
Pacific Northwest National Laboratory

J. Wise
Pacific Northwest National Laboratory

B. Gorton
Pacific Northwest National Laboratory

ABSTRACT

Law enforcement stakeholders use Sentry-SECURE to elevate situational awareness, which is critical to the protection strategies that safeguard radioactive materials. The Office of Radiological Security (ORS) uses these strategies to partner with stakeholders – government, first responders, and the material licensees – to protect radiological assets around the world. The development of a Cloud-enabled alarm monitoring architecture facilitates high-priority alarm and video signals reporting directly to an identified stakeholder via the technology's two data-consumption mechanisms, platform integration and mobile applications. This work presents the Sentry-SECURE beta test completed in March 2021 with a prominent law enforcement agency in Maryland, United States, and a network of disparate radioactive material licensees. Lessons learned, successes, and persistent challenges are summarized. Conclusions drawn from the beta test were used to inform and prepare additional law enforcement stakeholders for follow-on deployments scheduled for 2021 and 2022.

INTRODUCTION

Technology can be a powerful asset to the law enforcement community. Technology can also introduce unnecessary frustration, create noise, and be a drain on resources when not properly designed or implemented. In early 2021, development of a new, Cloud-hosted security technology was completed. The project provides a new capability known as the Sentry-RMS Communications and Response (Sentry-SECURE) feature deployed to a Sentry Remote Monitoring System (Sentry-RMS). Its objective is to promote situational awareness among stakeholders responsible for securing high-activity radioactive materials. Such stakeholders include, but are not limited to radiation safety officers, on-site security staff, and members of law enforcement. This paper summarizes the Sentry-SECURE beta test completed in March 2021. The work also provides insights as to the lessons learned, successes, and persistent challenges faced by the development team. Conclusions drawn from the beta test were used to inform and prepare for additional deployment projects with law enforcement stakeholders across the nation. These projects are scheduled for 2021 and 2022.

Office of Radiological Security

The development of Sentry-SECURE, and the parent system, the Sentry-RMS, is managed by the Department of Energy's Office of Radiological Security (ORS). ORS is funded by the U.S. Department of Energy and partners with organizations maintaining high-activity radioactive material to voluntarily enhance their security posture. Program support may include, but is not limited to, security focused hardware, software, policies, procedures, and training that contribute to the responsible management of critical assets containing radioactive materials of concern. These enhancements may directly and indirectly influence the physical, cyber, information, and operational security programs of the licensee. When developing new security technologies, ORS takes a comprehensive, multidisciplinary approach to consider each of the domains represented in Figure 1.

Figure 1. Primary security domains considered by ORS.

Summary of the Sentry-RMS

Figure 2: Photo of a Sentry-RMS

When organizations choose to partner with ORS, field assessments are completed to evaluate the existing physical protection system prior to making any recommendations. For sites with specific radioisotopes of concern in certain quantities, ORS may recommend the implementation of a security technology known as the Sentry-RMS. Figure 2 presents a visual of the unit in its standard configuration. The Sentry-RMS is a fully integrated, network-based security system with an onboard solid-state radiation detector, tamper alarms, continuous state of health, auxiliary inputs/outputs, and digital video assessment information that is communicated directly to stakeholders responsible for adjudicating priority alarms. The unit's design objective is to mitigate the insider threat as all detection and assessment capabilities remain operational around the clock. This means that security is provided without interfering with site or asset (device) operations. This is accomplished by using an alarm monitoring software known as an Operator Interface Software (OIS) client. Information from the Sentry-RMS is transmitted using a secure tunneling protocol over local or public network connections to the appropriate on-site and off-site locations maintaining the OIS monitoring client(s).

Specifically, the Sentry-RMS uses IPs [internet protocols] such as Hypertext Transfer Protocol Secure and Internet Protocol Security to provide secure and reliable communications. The Sentry-RMS can provide automated alarm notifications via its internally managed Simple Mail Transfer Protocol server with a secure interface. Also, all data at-rest and in-transit are secured by implementing the Advanced Encryption Standard to provide 256-bit symmetric encryption. Internally, the unit manages additional security controls such as firewalls, digital signature verification, and data redundancy mechanisms to assure its own confidentiality, integrity, and availability regardless of the environment to which it is deployed.

Sentry-SECURE platform summary

Sentry-SECURE is a feature of the Sentry-RMS that enables real-time, event-based alarm detection and assessment information to be communicated directly to stakeholders responsible for assessing priority alarms. Users at both ends of the technology have a strategic interest in this objective. Figure 3 is a simplified component diagram of Sentry-SECURE identifying RMS owners shown in black on the left side of the image. RMS owners represent site stakeholders, also known as the data owners or material licensees, that maintain high-activity radioactive materials that warrant protection and thus require the installation of a Sentry-RMS (e.g., universities, hospitals, research laboratories). RMS consumers are shown in orange on the right side of Figure 3. RMS consumers represent the response stakeholders who have a role in adjudicating high-priority alarms that may indicate a threat to the radioactive material.

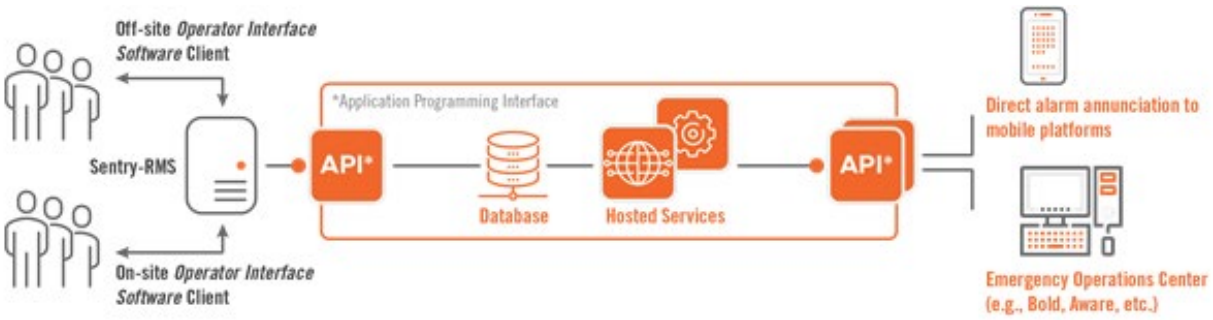

Figure 3. Sentry-SECURE platform component diagram.

RMS owners, primarily representative of site stakeholders (e.g., radiation safety officers, security directors), enroll their Sentry-RMS units and populate data fields necessary to inform a potential response effort. Examples of information an RMS owner may upload to the platform include asset characterization, site photos, maps, or personnel contact information. RMS consumers, primarily referring to law enforcement agencies providing an armed response capability, then augment the response information to fit their unique needs when executing their tactics, techniques, or procedures. Examples of information an RMS consumer might populate include detailed response procedures (e.g., how to abide by time-distance-shielding recommendations), personnel contact information, or rally point locations.

If a priority alarm is registered by the Sentry-RMS, an event stream is immediately, without human involvement, sent to Sentry-SECURE. The data are automatically forwarded to all data-consumption mechanisms configured by the authenticated and authorized RMS consumers. These data can be received by either an integrated alarm or event management platform, also called a computer-aided dispatch platform by many law enforcement agencies. Alarm event data can also report to the Sentry-SECURE mobile application, natively developed for both Android and iOS operating systems.

SENTRY-SECURE IN THE FIELD

The roots of Sentry-SECURE trace back to a white paper authored by response stakeholders in January 2019 that highlighted the need for a more efficient mechanism to share alarm event information between organizations. Discussions identified that a site, perhaps a university or hospital that detected a priority alarm using the Sentry-RMS did not have the on-site resources to engage or defeat a well-equipped, motivated adversary. By engaging local law enforcement, the responding force is authorized to use an appropriate spectrum of tactics, techniques, and procedures up to and including the use of lethal force. To best prepare the responding force to achieve a protection strategy of containment, it is critical that they be informed with strategic information including:

- Alarm event type
- Time
- Location (including site/campus, building, and room information)

- Assessment imagery (still photos and video) before and after the event
- Facility and area maps and diagrams
- Text-based information that may detail time, distance, or shielding principles important when dealing with radioactive materials.

Prior to the deployment of Sentry-SECURE, some of the above information was shared via phone call from the site's resident security force to a local law enforcement dispatch center. However, this approach does little to provide the officer in the field with enough information to achieve a status of tactical readiness to engage an adversary committed to carrying out acts of terrorism involving high-activity radioactive materials. There was also the risk of information being miscommunicated as staff from different roles and organizations were required to communicate sensitive information on short notice and in times of high stress. With a fully developed and deployed Sentry-SECURE mobile application receiving the enhanced situational awareness described above, the officer in the field is now well-informed and better prepared to engage the oppositional force in significantly less time with significantly more information.

Development summary

At the onset of beta test in March 2021, Sentry-SECURE was fully developed but had not yet seen concurrent connections from and to multiple stakeholders. It is important to understand that Sentry-SECURE is effectively an infrastructure that connects RMS owners to RMS consumers once both user groups have been authenticated and authorized to the other stakeholder. Once approved by the user at the other end of the technology, a connection is established that allows for the situational awareness to be shared from RMS owner to RMS consumer. To support this sort of agile infrastructure, the development team had to identify the technical requirements, design the architecture, configure the microservices, complete over a dozen types of testing, and overcome a seemingly endless litany of other challenges that presented themselves throughout the two-year development effort.

However, the greatest challenge was to establish a balanced design that addressed the operational, security, and sustainability challenges the stakeholders will face upon fielding the technology. From the operational perspective, one must consider the end user. When adjudicating a possible threat scenario, members of law enforcement are faced with a low probability, but high consequence event. This means that upon receipt of an alarm, the situation must be responded to as if it is a confirmed threat scenario. Public safety may hang in the balance. From the security perspective, both cyber and physical security considerations were embedded into the earliest of design considerations, prioritizing integrity, availability, and confidentiality. This was challenging because advanced cybersecurity controls were necessary to enable the technology to live in the wild but must be implemented in a way that can be wielded by those who are not cyber experts. Furthermore, the development effort was completed with sustainability held as a priority. As a result, it was necessary to develop a lightweight and agile platform, with high availability, that can scale up or down to adjust to user demand. This design consideration optimizes resource consumption,

primarily referring to the minimization of operating costs. This is an ever-present constraint when endeavoring to develop a new technology.

Beta test objective

The objective of the beta test was to implement Sentry-SECURE across the identified RMS owner and consumer organizational pairings to verify that functional and performance requirements were satisfied when deployed to the field. Technical and project support was provided by Pacific Northwest National Laboratory staff, the development contractor, and embedded commercial security vendors. Specifically, such support included the installation, configuration, testing, and training to deploy Sentry-SECURE components in the field. Once placed in the hands of potential future users, the development team observed how the technology was used, or misused, and garnered as much feedback as possible. Feedback included user experience, technical, operational, and design relevant comments, observations, questions, deficiencies, bugs, and frustrations.

Stakeholders involved

The Sentry-SECURE beta test was supported by nine organizations that can be grouped into two categories – [1] support organizations and [2] RMS owners and RMS consumers. Table 1 shows the breakdown by category.

Table 1. Sentry-SECURE Beta Test.

Support Organizations	***RMS Owners and RMS Consumers***
Office of Radiological Security	Biotechnology company
Development Contractor	Radioactive material shipping company
Security Vendor	Pharmaceutical research and development company
Embedded IT Organizations	Law Enforcement Agency
Cloud provider	

For security and informational sensitivity reasons, the specific organizations who participated in the beta test have been kept private. However, Table 2 shows the devices used during the beta test.

Table 2. Mobile Devices used in Beta Test.

Qty.	***Product***	***Platform***
2	Samsung - Galaxy S10+	Android
2	Kyocera DuraForce Pro 2	Android
2	Samsung - Galaxy Xcover PRO	Android
1	Samsung - Galaxy Tab S5e	Android
1	Samsung - Galaxy Tab S6	Android

Qty.	*Product*	*Platform*
1	Apple - iPad Air (10.5-inch)	iOS
1	Apple - iPhone 11 Pro	iOS
1	Apple - iPhone SE	iOS
1	Apple - iPad Pro (12.9-inch)	iOS

In all cases, the devices complied with a technical requirement that the Sentry-SECURE mobile application operate on Android Version 6, and newer, and Apple iOS Version 10, and newer. This was prescribed to allow reasonable backward compatibility while not limiting the development team from more modern capabilities deployed by the mobile device manufacturers in recent operating system (OS) releases.

Execution of beta test and takeaways

The scope of beta test spanned a two-week period. The first week (five working days) was allocated to initial configuration, training, and deployment related activities. The development team held all scheduled meetings in the mornings to allow for more dynamic interactions in the afternoons with specific stakeholders – vendors, IT staff, among others. In effect, this allocated time to meet the known, required benchmarks in the mornings while also remaining agile to accommodate questions, discussions, and/or implement the work as necessary in the afternoons. This approach proved to be key to overcoming challenges inherent to testing a new technology. The second week was allocated for stress testing, use case testing, and allowing for the end users to complete tests unique to their own organizations. In several cases, the stakeholders returned unsolicited but well documented, well executed performance tests. This was received as evidence of the stakeholders' excitement to interface with the new technology.

Included below is a topical summary of the content covered during the first week of the beta test:

- Introduce project and deliver overview
- Configure network infrastructure to support the Sentry-SECURE feature of deployed Sentry-RMS units
- Update Sentry-RMS firmware for each unit being registered to Sentry-SECURE with the latest release
- Create RMS owner and consumer accounts
- Register Sentry-RMS unit(s) within the RMS owner account
- Complete RMS owner profile. This entails uploading site-specific data provided by the RMS owner including alarm response instructions, site images, site maps, site diagrams, and contact information
- Complete RMS consumer profile. This entails uploading organization-specific data provided by the RMS consumer to augment the existing data

- Create and provision Sentry-SECURE mobile application users
- Download and provision the Sentry-SECURE mobile application for the identified users

The content covered during the second week of the beta test included RMS owner and consumer simulated events, supporting user runtime, user-defined testing, and rolling back Sentry-RMS firmware to pre-beta firmware versions. By the conclusion of the beta test, all stakeholders participated in structured testing as well as unrestricted use of the Sentry-SECURE mobile application. Figure 4 presents still images of what the stakeholders interfaced with once their accounts were provisioned and populated. For each RMS owner-to-RMS consumer connection, site-specific naming conventions, standard operating procedures/alarm instructions, photos and diagrams, and other forms of data were uploaded to Sentry-SECURE. During this period of use, the mobile application was demonstrated to be intuitive. User training provided by the development team increased user proficiency while also establishing an elevated, uniform level of situational awareness among the authenticated and authorized users. Such users included regulatory, operations, management, security, and law enforcement staff. Users also appreciated what was described as a professional look and feel of the mobile application, providing efficient movement between and within connected RMS owner-to-RMS consumer connections.

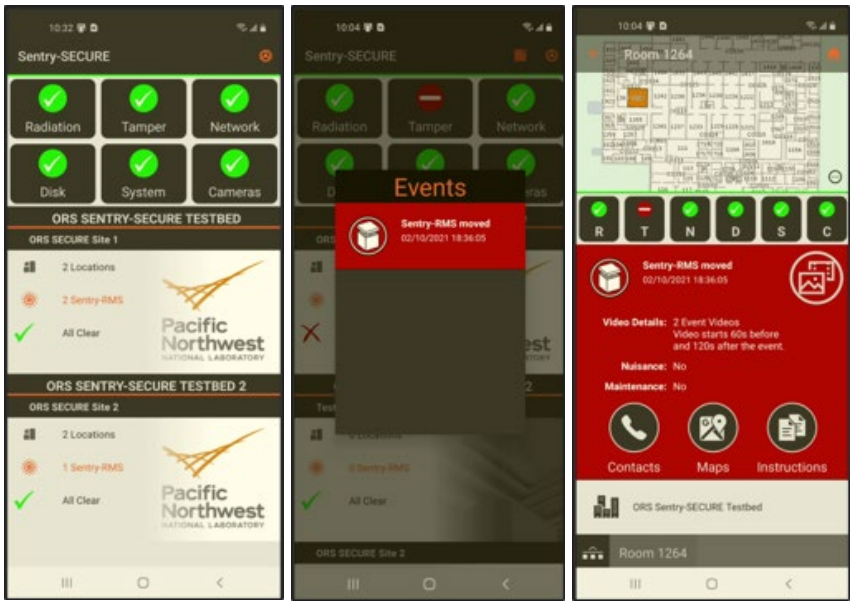

Figure 4: Sentry-SECURE mobile application screens.
From left to right; [a] homescreen with no alarm conditions, [b] active alarm event prompt, [c] expanded alarm event screen

After the Sentry-SECURE beta test ended, including the deactivation of all user admin accounts, the development team compiled the feedback. Feedback was distilled down into two primary categories – bugs and feature requests – and assigned a qualitative priority ranking of high or low. While both were considered important, only the actions identified as bugs warranted immediate resolution to close the contracted development scope. The final bug tracker contained 19 actions, 10 of which are listed below in Table 3. It is noteworthy that all 19 actions dealt with aspects of the graphical user

interface or user design while zero presented any known security vulnerabilities. For a technology development of this complexity, the collective development team, consisting of the development contractor, Cloud service provider, and program staff, were both extremely encouraged by the qualitative and quantitative metrics associated with the beta test.

Table 3: Sentry-SECURE Bug Tracker

List item	*Description*
1	Must be on the main page to start the help; change to show current page upon clicking help. Content is missing from Help prompts
2	Export request should include both image stills and alarm video
3	When troubleshooting the RMS owner-to-consumer pairings, is there a more prescriptive description for the Me/Them/Effective tags? This feels abstract and was not understood by the beta test participants
4	Upon initial bootup of the mobile app, all State of Health (SOH) showed “N”; “N”s cleared after restart
5	At the room level, SOH is truncated and does not show all icons (“C” is cut off)
6	The SOH prompt is not refreshing to display the latest update; when the SOH box is already being displayed, the updated alarm status is not being shown. Repeated twice and saw same bug
7	The app presenting bug when attempting to retrieve videos directly after alarm annunciation, but before videos arrived. Clicked media button causing app to crash, repeated behavior and experienced same failure
8	Specific events presenting lag from phone to app or app to phone; reference notifications center parameters for consecutive events
9	Still images were not sent during the period of a communication loss event upon comms returning to normal (images are not queued and provided retroactively)
10	Sentry-SECURE status not displaying Bad within Event Viewer tab during comm loss

Table 4 contains the 10 of the 17 points of feedback that were classified as user feature requests. These actions have been assigned a priority and are being considered for future development.

Table 4: Sentry-SECURE Feature Request Tracker

List item	*Description*
1	Display Org and Account Admin name on all portal screens
2	Confirm Save command upon successful write via user prompt
3	Enable more efficient data entry for instruction set (alarm SOPSs)

List item	*Description*
4	Ellipses (when expanding the image within the mobile app) is masked depending on the color of the image. Alter ellipses to be two-toned to always present icon
5	Add a reference timestamp to timing of event/clock on the video
6	Provide for an image preview of what has been loaded (e.g., add magnifying glass to portal)
7	Dump log data export into readable format, e.g., .csv file
8	Enable app to display whether the monitoring client has acknowledged event or if it is active
9	Add ability to look at historical/past events via the mobile application (+History button)
10	Enable a test event to be sent to mobile app users – automatically/pre-scheduled and on-demand

Challenges presented by mandatory remote work environment

Public health concerns stemming from the COVID-19 pandemic persisted throughout calendar year 2020 and did not appear to be lessening in the early months of 2021. As a result, the project team, in agreement with the stakeholders identified above, elected to move forward in an entirely remote capacity. Put another way, the planning and execution of the Sentry-SECURE beta test was completed without physical interaction among the stakeholders identified above. Microsoft Teams was the primary tool used to facilitate both structured and dynamic meetings, discussions, trainings, configuration sessions, testing, and deployment related activities. From the administrative side, logistics were simplified as no travel was required – staff were able to attend events from the comfort of their own accommodations. However, using a technology intended for virtual engagement, for which many users are not proficient with, to roll out a newly developed technology intended for kinesthetic use is far from ideal.

As a result, the project team was forced to adapt and find ways to demonstrate proper use of a tactile tool, Sentry-SECURE, without modeling or observing physical touch. To layer in additional challenges such as network instability, lack of familiarity with Microsoft Teams (or any collaboration software), disparate device hardware, and conflicting virtual attendance, the path to a successful beta test was far from what was originally intended. Thankfully, all staff including the RMS owners, RMS consumers, and support organizations remained agile, collaborative, and eager to move forward despite the unforeseen challenges. Because of their efforts, Sentry-SECURE was able to garner valuable feedback to conclude the development effort.

CONCLUSION

Prior to exposing Sentry-SECURE to the wild, a thorough function and performance test was necessary. In March 2021, a beta test completed with a prominent law enforcement agency in Maryland, United States, and a network of disparate RMS owners. As confirmed over the two-week test, Sentry-SECURE enhances the security of high-activity radioactive materials by increasing the

situational awareness shared between stakeholders and across organizations critical to adjudicating priority alarm events. Development of the Sentry-RMS Cloud-enabled architecture enables high-priority alarm and video signals to report directly to an identified stakeholder's alarm and event management platform, such as local law enforcement or site management. This reporting occurs in parallel to the site executing their alarm adjudication procedures. As demonstrated during the beta test, the technology also transmits alarm event and video signals directly to a first responder's mobile device.

At the conclusion of the beta test, both successes and lessons learned were identified that greatly informed the remaining development tasks. While executed amid unforeseen challenges that hampered much of the security industry, the project satisfied its mission objective, met all technical requirements, and operated within its defined budget and schedule constraints. The beta test also failed to identify any critical flaws, or missed requirements, despite a pointed effort to do exactly that. Specifically, the beta test identified 19 bugs to be addressed in the near term and 17 feature requests to consider for future development. Additional takeaways were captured to inform and prepare the development team for production deployments starting in 2021 and scheduled out through 2022.

ACKNOWLEDGMENTS

The staff involved in supporting this scope would like to express their appreciation for the Leadership Team within the Office of Radiological Security program as well as the Portfolio Leads for the Response, RMS, and Cybersecurity tasks. The continued guidance and support serve as the foundation for new and innovative capabilities to enhance the strategic partnerships between law enforcement stakeholders, high-activity radioactive material licensees, and security practitioners across the nation.