Communications of the IIMA

Volume 11 | Issue 3 Article 5

2011

Developing a Metrics Framework for the Federal Government in Computer Security Incident Response

Vincent Sritapan
California State University San Bernardino

Walter Stewart
California State University San Bernardino

Jake Zhu
California State University San Bernardino

C.E. Tapie Rohm Jr.
California State University San Bernardino

Follow this and additional works at: http://scholarworks.lib.csusb.edu/ciima

Recommended Citation

Sritapan, Vincent; Stewart, Walter; Zhu, Jake; and Rohm Jr., C.E. Tapie (2011) "Developing a Metrics Framework for the Federal Government in Computer Security Incident Response," *Communications of the IIMA*: Vol. 11: Iss. 3, Article 5.
Available at: http://scholarworks.lib.csusb.edu/ciima/vol11/iss3/5

This Article is brought to you for free and open access by CSUSB ScholarWorks. It has been accepted for inclusion in Communications of the IIMA by an authorized administrator of CSUSB ScholarWorks. For more information, please contact scholarworks@csusb.edu.

Developing a Metrics Framework for the Federal Government in Computer Security Incident Response

Vincent Sritapan
vsritapan@gmail.com

Walter Stewart
wstewart@csusb.edu

Jake Zhu
jzhu@csusb.edu

C. E. Tapie Rohm Jr.
trohm@csusb.edu

California State University San Bernardino, USA

ABSTRACT

As technology advances and society becomes more dependent on information technology (IT), the exposure to vulnerabilities and threats increases. These threats pertain to industry as well as government information systems. There is, however, a lack in how we measure the performance and create accountability for computer security incident response (CSIR) capabilities. Many government organizations still struggle to determine what security metrics to use and how to find value within these metrics. To fill this apparent gap, a metrics framework has been developed for incident response to serve as an internal analysis, supporting continuous improvement in incident reporting and strengthening the security posture for an organization's mission. The goal of this metrics framework for CSIR aims to provide a holistic approach towards security metrics, which is specific to incident reporting and promotes efforts of more practical and clear guidelines on measuring the computer security incident response team (CSIRT). An additional benefit to this project is that it provides middle management with a framework for measuring the results of incident reporting in a CSIR program.

INTRODUCTION

As technology becomes more prevalent and reliance on IT expands, the exposure to vulnerabilities and threats increases. Malware, social engineering, and zero day attacks have evolved to outpace current IT security controls. In the *Cyberspace Policy Review*, the United States (US) acknowledged its need for more reliable, resilient, and trustworthy digital infrastructure for the future (White House, 2009). Realizing the need for enhanced cyber security and information security management criteria, federal regulations have mandated the capability, provision, and notification for cyber security incidents ("Federal Information Security Management Act of 2002" (FISMA), 2002). The U. S. Department of Homeland Security's

Computer Emergency Readiness Team (CERT) requires incidents by category type for computer security incident response to be reported within specific timeframes (n.d.). The requirement creates an audit trail for the purpose of awareness and collaboration. However, the main concern drawn from this initiative is accountability. How can an organization follow alerts, check validations, and track remediation efforts? What controls are in place to determine if appropriate reporting methods exist and are being used properly? How can an organization verify that requirements are being met? Additionally, in the event that reporting methods are confirmed, how can organizations measure performance? By examining the federal work space, it is apparent that federal agencies are required to adhere to the *Federal Information Security Management Act (FISMA)* (2002), Office of Management and Budget (White House, n.d.) directives, and the U. S. Department of Homeland Security's (DHS, 2011) timeframe reporting requirements. In this effort the metrics framework for incident response has been developed to serve as an internal analysis, supporting continuous improvement in incident reporting and strengthening the security posture for an organization's mission.

REVIEW OF THE LITERATURE

Since the early 1990s, from the Defense Advanced Research Project Agency's (DARPAs) push for CERT/CC to the establishment of US-CERT by DHS, the federal government has initiated multiple efforts for cyber security and CSIR (Ellis, Fisher, Longstaff, Pesante, & Pethia, 1997; White House, 2009; Wilshusen, 2011). The efforts for accountability have been established under FISMA (2002), OMB directives (White House, n.d.), and Inspector General (IG) audits (U. S. Department of Homeland Security, Office of the Inspector General, 2010). However, the effectiveness for measuring performance and compliance still remains a controversy (U. S. Government Accountability Office, 2010; Hopkins, 2009). Audits have continually evolved from yes and no questions to how many and why (B. Gorsen, Personal Communication, 2010). Efforts to effectively account for programs such as CSIR have become an area of concern.

Measurement Types for Computer Security Incident Response

There is a wide variety of reputable publications illustrating measurement types and metrics for CSIR. In the NIST Special Publication 800-55 Revision 1, Chew, Swanson, Stine, Bartol, Brown, and Robinson (2008) defined measurement types for information security as implementation, effectiveness/efficiency, and impact. The authors established that these are measurement types but they are actually purposes or the drive for measuring information security. In another NIST publication, NIST Special Publication 800-61 Revision 1, Scarfone, Grance, and Masone (2008) suggested possible metrics for CSIR as the number of incidents handled, time per incident, objective assessment of each incident, and subjective assessment of each incident. These metrics are very practical but suggest only a small portion of possible metrics and measurement types for measuring CSIR. In another technical report from Carnegie Mellon's Software Engineering Institute (SEI), Dorofee, Killcrece, Ruefle, and Zajicek (2007), measured incident management based on common functions and processes within CSIR work flow. Their approach to measure CSIR capabilities, also stated as incident management capabilities, is based on evaluating business functions. This form of measuring CSIR looks primarily at overall performance, while attempting to apply its own scoring rubric to business functions within CSIR. An additional measurement type or scale was defined by Allen and Davis (2010) as nominal, ordinal, interval, and ratio. These are specific measurement types based on possible mathematic operations and measurable service types for CSIR. Lastly, another insight into the types of measurements for CSIR was suggested by Gartner analyst and metrics expert Jeffrey Wheatman (personal communication 2010) as cost, time, and quality for any metric. Wheatman's statement of cost, time, and quality for metrics is based on common sense and practical knowledge. Compared to the various types of measurement or metrics suggested from other authors, Wheatman's approach to measurement types of security metrics in CSIR is holistic because it provides the flexibility to measure for any purpose or objective.

THREE TYPES OF MEASUREMENTS

Measurement of cost, time, and quality are evident in business as the 'iron triangle', but the terms are used in a different context for this metrics framework for CSIR. Atkinson (1999) reviewed the measurements of cost, time, and quality as it pertains to project management. The tradeoffs that exist within a project are similar to a cost benefit analysis that is useful to project management. However, for this metrics framework for CSIR, Wheatman's (personal communication 2010) basic concept of cost, time, and quality is used for the three measurement types. Allen and Davis (2010), in a technical report, agreed with the definition of cost as a value of money. The evaluation of cost is taken in a literal sense as encompassing only financial value, meaning dollars and cents. Scarfone, Grance, and Masone (2008) referred to time as the time an incident occurs to the time it is resolved. The importance of time as a measurement is referenced to timeframe or duration of an incident. As for quality, West-Brown, Stikvoort, Kossakowski, Killcrece, Ruefle, and Zajicek (2003) identified quality as quality parameters that are common between services or functions. Quality is defined as good or bad based on how well the expectation level and set parameters are met. The three types of measurements for CSIR exist throughout aspects of publications regarding CSIR.

Security Metrics

There are numerous publications for security metrics, but there is not one governing source that combines the efforts of creating security metrics. Chew, Swanson, Stine, Bartol, Brown, and Robinson (2008) provided a comprehensive guide for creating measurement for information security programs. Additionally, the Center for Internet Security Community (CISC, 2010) has derived 28 metric definitions that apply broadly to seven information security programs, such as incident management, vulnerability management, patch management, application security, configuration management, and financial metrics. They emphasized providing common metrics and definitions that support measurement of important business functions. In addition, Jansen (2009) indicated the direction of security metrics research going towards formal models and security measurement and metrics, historical data collection and analysis, artificial intelligence assessment techniques, practical concrete measurement methods, and intrinsically measurable components. Security metrics is on the path stated by Jansen and evidence of more practical and formal models are demonstrated by the effort of this project.

Objective Driven Measurements

The purpose of a measurement is to serve a particular objective. Chew, Swanson, Stine, Bartol, Brown, and Robinson (2008) stated that organizations should define the scope of their information security measurement program based off strategic goals and objectives among other things. In an interview with Barbara Gorsen (personal communication, 2010), Gorsen stated that objectives need to be clearly defined before pursuing measurements within CSIR. Allen and Davis (2010) identified the importance of establishing objectives as a basis for measurements. Measurements, therefore, are derived from objectives to validate the reason for assessment. Lastly, Alberts, Allen, and Stoddard (2011) discussed, in *Security Measurement and Analysis*, mission-objective-driver protocols that drive analysis. This metrics framework clearly identifies objectives as an essential criterion to the development of measurements and to drive the basis for evaluation.

PROCESS FLOW IDENTIFICATION

Identifying incident response capabilities process flow provides a map of how an incident is handled from start to finish. In a technical report from Carnegie Mellon’s SEI, Alberts, Dorofee, Killcrece, Ruefle, and Zajicek (2004) defined incident management processes for CSIRTs using a process model. The process model for incident management outlines and documents process activities to aid in benchmarking. The common processes for evaluation are stated as: Prepare/sustain/improve (Prepare), protect infrastructure (Protect), detect events (Detect), triage events (Triage), and respond (Alberts et al., 2004). Additionally, recommendations for creating a CSIRT by Scarfone, Grance, and Masone (2009) addressed the need for developing incident response procedures that cover all the phases of the incident response process. There is a direct correlation between understanding and documenting processes and benefiting from it when measuring CSIR capabilities. Chew, Swanson, Stine, Bartol, Brown, and Robinson (2008) stated that developing performance measures in advance during the creation of a security program allows for the benefit and ease of security metrics. Understanding the processes for improvement is again stated by Dorofee, Killcrece, Ruefle, and Zajicek (2007) as essential for metrics evaluating incident management capabilities. Identifying and being aware of processes enables for more accurate measurements and offers process improvement opportunities.

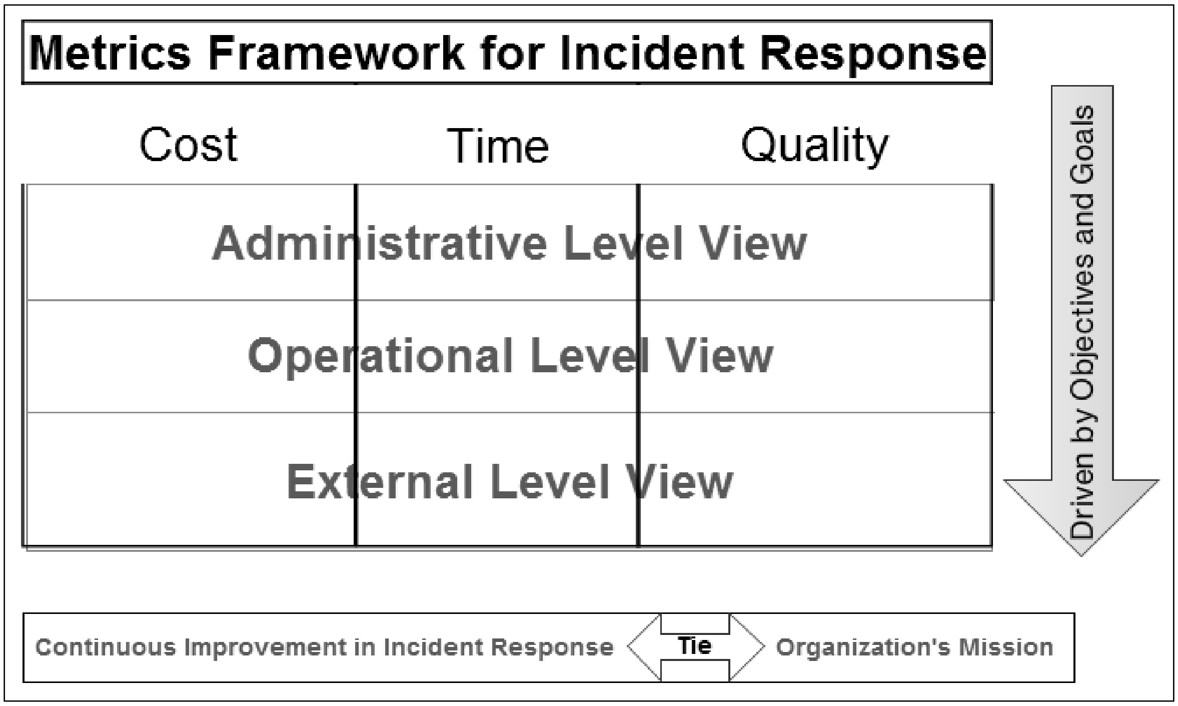
AUDIENCE BASED METRICS

The notion of audience based measurements derives from professional experience, personal communication, and from the idea that different perspectives exist. Gartner analyst Michael Smith (personal communication, 2010) discussed the importance of understanding the audience and their expectations, and their needs associated with their position as a stakeholder within CSIR. Additionally, Niven (2008) addressed the four perspectives that exist for a balanced scorecard. This includes the customer perspective, internal process perspective, financial perspective, and employee learning and growth perspective. The concept of different views as a basis for metric requirements was essential in the development of audience based metrics.

Tying Security Metrics to Organization's Mission

Chew, Swanson, Stine, Bartol, Brown, and Robinson (2008) stated that federal agencies need to link information security with enterprise strategic planning. West-Brown, Stikvoort, Kossakowski, Killcrece, Ruefle, and Zajicek (2003) also stated that CSIRTs mission must complement the organization's mission. The point of information security efforts is to support the agency's overall goals and objectives. Additionally, in an interview with Gartner analyst Michael Smith (personal communication, 2010), Smith noted that the point of CSIR is to assist in the agency's mission. Therefore, measuring CSIR should follow suit by looking at ways to improve CSIR capabilities to support the agency's mission. Tying security metrics to the organization's mission is vital to the success of security metrics for CSIR (see Figure 1).

Figure 1: Metrics Framework for Incident Response.


Metrics Framework for Incident Response
Cost
Time
Quality
Administrative Level View
Operational Level View
External Level View
Driven by Objectives and Goals
Continuous Improvement in Incident Response
Tie
Organization's Mission

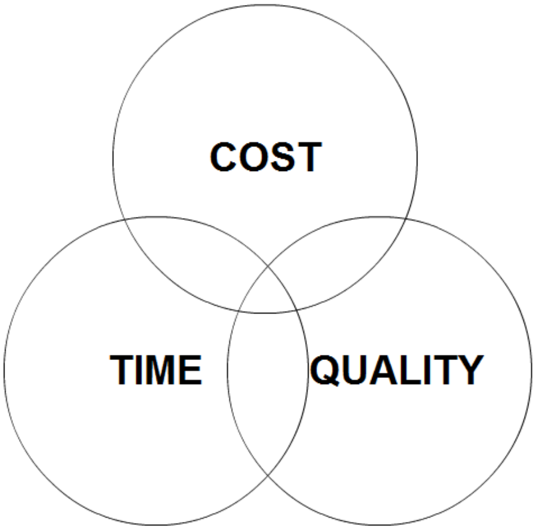
Steps to Use the Metrics Framework

Before using the metrics framework one needs to have an understanding of one's agency's CSIR capabilities, its maturity level, and what types of measurements exist for evaluating CSIR. The first step is to determine what is the objective and purpose for measuring CSIR capabilities. The second step is to select what measurement to use based off the determination of the objective and purpose. The third step requires the identification of all data sources and responsible parties. Then the measurement is conducted with the appropriate approval from management. The fourth step is to tailor the results specific to the needs of the audience base, giving consideration to viewing requirements. The fifth step is to assess the results and determine if action is needed. The sixth step is to take action, if needed, and review all previous steps that have been taken.

THREE TYPES OF MEASURES FOR COMPUTER SECURITY INCIDENT RESPONSE

Three types of measures that exist for evaluating IR include cost, time, and quality (see Figure 2) (J. Wheatman, personal communication, 2010). These three measures provide a holistic approach towards evaluating efficiency, effectiveness, and implementation in an IR program. When evaluating incident reports, these three measures can overlap by comprising a mixture of two or three measures. For example, when using the metrics framework to evaluate compliance for timeframe reporting the result may require management to consider implementing changes that impact the cost of the IR program. The cost benefit analysis for decreasing reporting time to meet timeframe requirements is a measurement of quality. This involves all three measurement types to address compliance. Depending on the purpose for measuring IR, these three measurement types will be the foundation to evaluate and measure a CSIR program.

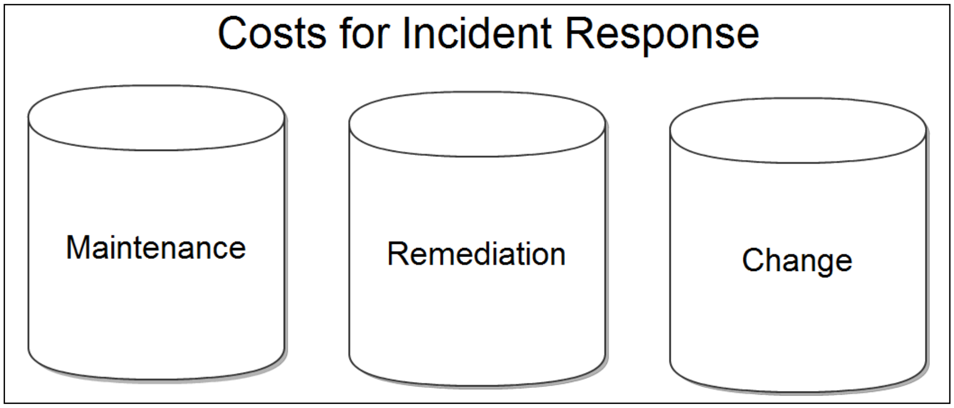
Figure 2. Three Measurement Types for Incident Response.



Cost in CSIR is determined based on three areas: 1) the cost to maintain IR capabilities, 2) the cost to remediate an incident, and 3) the cost to implement change in an IR program (Rezmierski, Deering, Fazio, & Ziobro, 1998) (See Figure 3). Please note that cost for this metrics framework deals only with financial cost. There are existing formulas (See Appendix B) that aid in evaluating IR and offer standardized expressions to make IR evaluations more consistent. When evaluating costs for IR, the more entities that are identified and assigned costs, the more accurate the cost measurement will be. For tangible items, cost is easier to assign. But for intangibles such as reputation and trust it becomes much harder to assign a dollar amount. The criteria for evaluating cost for IR requires identification of the three cost areas and the ability to continually assign related costs as new costs are identified.

The cost to maintain CSIR capabilities and services include direct and indirect costs that can be attributed to CSIR operational costs. From an accounting perspective the cost of direct labor, direct material, and applied overhead costs should be considered (Brewer, Garrison, & Noreen, 2009). Activity based costing method for calculation is suggested. However, the trade-off to more accurately assigned activity costs is the time and money needed to discover the cost of each activity. The best way to determine cost to maintain CSIR is to evaluate the need to measure and how much the organization is willing to pay in order to obtain accurate cost estimates.

Figure 3: Cost Types for Incident Response.

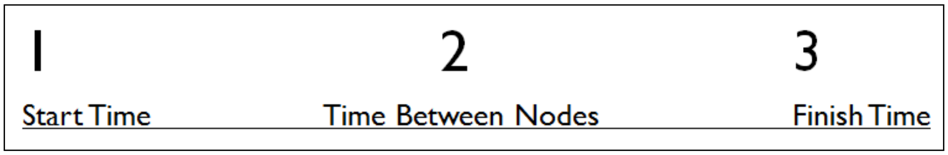


The cost to remediate varies depending upon the incident and the methods chosen to remediate. But for this metrics framework it is important to find common incidents that have relatively similar financial costs. Although costs will vary, it is crucial that all methods of remediation attribute a financial cost when applicable. As noted before, intangibles like trust and reputation do not always have an associated financial cost. Therefore, it is important to look at costs for either costs savings or improvement in remediation efforts.

Implementation costs are financial costs attributed from the impact of making change to CSIR capabilities. The cost to implement change depends on both the cost to maintain services and the cost to remediate. A cost benefit analysis approach is recommended for determining implementation costs (Xie & Mead, 2004). The importance of implementation costs are determining whether or not making change is worth the financial costs, given the desired outcome and the likelihood it would occur.

The importance of measuring time for CSIR is the duration between activities and the total time it takes to resolve an incident. This deals with points of time and the lengths of time in between points. In particular there can be two or more points that exist within a CSIR event. The three points of time for an incident include: 1) Start Time, 2) the Time-in-Between, and 3) the Finish Time (see Figure 4).

Figure 4: Time Measurement Points for Incident Response.



Start time usually is the time the incident is reported. It is the first recorded and realized moment that an incident has occurred. This statement for start time is probably the most important aspect of measuring time for CSIR because of the discrepancies that exist within a FISMA or IG audits. As shown in Chapter 1, the timeframe reporting requirements US-CERT states broad to strict reporting times depending on the different incident categories. Therefore, it only makes sense that the time to report only starts when an incident is reported and is realized, meaning the first time it is reported at the level being considered.

Time-in-between deals with the many nodes an incident goes through as it is resolved by one or many entities. The finish time can either be the time the incident is reported as resolved or the time the incident report is closed out. The structure for measuring time depends on how an agency keeps its timestamps and what aspect of time it is trying to evaluate. Time in the sense of IR is all about how long. Determining how long offers the ability to gauge performance. It allows agencies to determine if changes are needed and how changes can affect time.

Quality is self-determined that can be subjective or objective or both depending on the measurement conditions (Scarfone, Grance, & Masone, 2008). An organization is able to interpret the results of an IR measurement and gauge whether the results are good or bad. Statistics such as counts for incidents initiated, unresolved, or resolved are interpreted based on the priority and values of the organization. A high number of reported incidents may be seen as a good thing because it shows that people are reporting incidents as they occur. However it could also mean the agency's security controls are not doing their job. Or, adversely, a low incident count could reflect that security controls are working and there are a less number of incidents occurring. However, this could just as well be the agency not reporting because of fear of showing that too many incidents are occurring. Depending on the agency's priorities and goals, any particular moment can drastically effect the interpretation of IR results and the value that exists in that information. Quality is thus self-determined and put into the interpretation of the agency based on where they find value in the information.

Objective-Driven Measurements

It is important to establish the objective for maintaining a metric before introducing IR evaluations to an audience. This allows the audience to relate how measuring performance of an IR program supports the organization's mission. As identified in NIST Special Publication 800-55, security metrics must be driven by goals and objectives (Chew et al., 2008). The audience must understand the objectives for an IR metric in advance to understand why measurement of a CSIR is being conducted (Alberts et al., 2011).

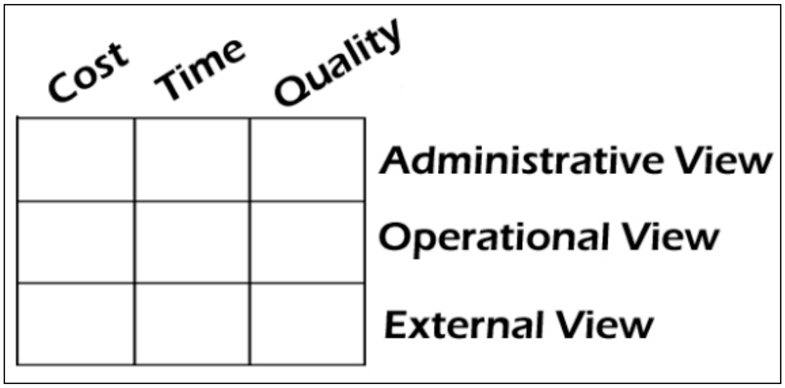
This component of the metrics framework is essential in the determination, selection, and presentation for measuring CSIR capabilities. Determining objectives is the first step before selecting security measurements for a CSIR program. A crucial part of determining objectives for security measurements is to evaluate organizational needs and the mission of the organization.

By deriving security measurements from objectives and goals, the results from the metric can be meaningful. Objective driven metrics enable the entity that is conducting the measurement to bring value to the organization using the results from the metric evaluation. Clearly stating the objective and goal of the measurement before selecting what to measure offers guidance into what should be measured and explains to the audience why it is being measured in the first place. Therefore, objective driven measurements are essential to the success of conducting security metrics for a CSIR program and gives consideration to organizational measurement concerns.

AUDIENCE BASED MEASUREMENTS

As shown in Figure 5, there are three identified audience groups for the intended user of the metrics framework: 1) administrative, 2) operational, and 3) external. Since the intended user is middle management, the audience meant for the security measurement of a CSIR involves upper management, CSIRT staff, and auditors. Each audience group has its own specific needs. While their needs may overlap, each group's purpose for viewing the results of a CSIR security metric is quite different.

Figure 5: Audience Based Measurements.



The administrative level view is based on middle to executive level management. Stakeholders at the administrative level view may include the chief information officer, chief financial officer, chief technology officer, chief information security officers (CISOs), associate CISOs, and directors of bureau CSIRTs. These positions within an agency have relatively large amounts of responsibility for the agency and high level decision making powers, therefore, this group may only be interested in high level information and may want everything synthesized for the purpose of making high level decisions.

The operational level view includes those who are on the front lines actually identifying and resolving the incident. It includes the technical staff that may want the detailed information to find problems within the CSIR processes. Stakeholders at the operational level view includes CSIRT managers, CSIRT analysts, CSIRT operators, and all other CSIRT personnel that have direct contact with the CSIR processes at the bureau level. It is important to understand the role of stakeholders at the operational level because it offers insight into the expectation of security metrics and metric results. Stakeholders at the operational level may be interested in the cost and or time to respond to an incident within the bureau CSIRT.

The external level view is for auditors, those outside the CSIR program that need an assessment into measuring CSIR performance. Stakeholders at the external level view include FISMA auditors by DHS, IG auditors, and all other entities looking at the performance measure of CSIR capabilities from outside the agency. This may include the IG of an agency who would technically be inside the agency, but because of their role they are considered at the external level view. The importance of grouping this type of audience into the external level view is because their needs are specific to check for compliance against some specific standard, regulation, or mandate.

Understanding that the audience does matter and giving them consideration for the selection of security metrics for CSIR is important to the success of conducting any security metric. This is a critical aspect of the metrics framework because it offers the ability to identify measurements based on audience needs. Therefore, all of these views are important for selecting security metrics for CSIR and tailoring relevant IR metric results to the intended audience.

Tying Measurements to the Agency's Mission

Tying security measurements and its results to the agency's mission is a crucial segment for the metrics framework. This makes sure that measuring CSIR is not just for the sake of measurements. The reason CSIR exists is to benefit the agency's mission. This could mean passing an audit so the organization is able to continue its normal operations or responding to a reported incident that saves the agency time and money. Therefore, the importance of measuring CSIR is to prove that it supports and enables the agency to accomplish its mission. By describing in words how the measurement ties into the agency's mission, we can demonstrate the value within the CSIR program.

In order to tie the security measurement to the agency's mission, the purpose and objective needs to drive the actual security metric from the beginning. If done properly, the objective and purpose that drives the security measurement for CSIR will be restated and will serve as the bridge to demonstrate how the CSIR program supports the agency's mission. For example, a measurement is part of a series of measurements that is helping the organization prepare for an audit. Any objective can be stated as long as it supports the agency's mission. If the agency is aware of the measure and its support of the agency's mission, then the agency as a whole will understand the value behind CSIR capabilities.

Process Flow Identification

Process flow identification involves identifying the processes within CSIR capabilities. For a bureau, the process flow starts from the incident being reported/detected, to triaging, to remediating, to sustaining, and at some point reporting to the agency headquarters CSIRT. For an agency it is similar, except the agency reports to US-CERT. Depending on the makeup of the organization the process for notification and remediation will vary, as shown in Figures 6 and 7. Agency level process flows are illustrations of bureau level and agency headquarters level process flows for incident reporting. They illustrate the processes and functions within a CSIR capability. They show the methods of communication such as phone, email, and web portal. Important to note is that the process and makeup will vary at the federal government level, depending on the CSIRTs position within an agency. Notably the accuracy and greater capabilities in a CSIR program will depend on the maturity level of the CSIRTs.

Figure 6: Bureau Level Process Flow.

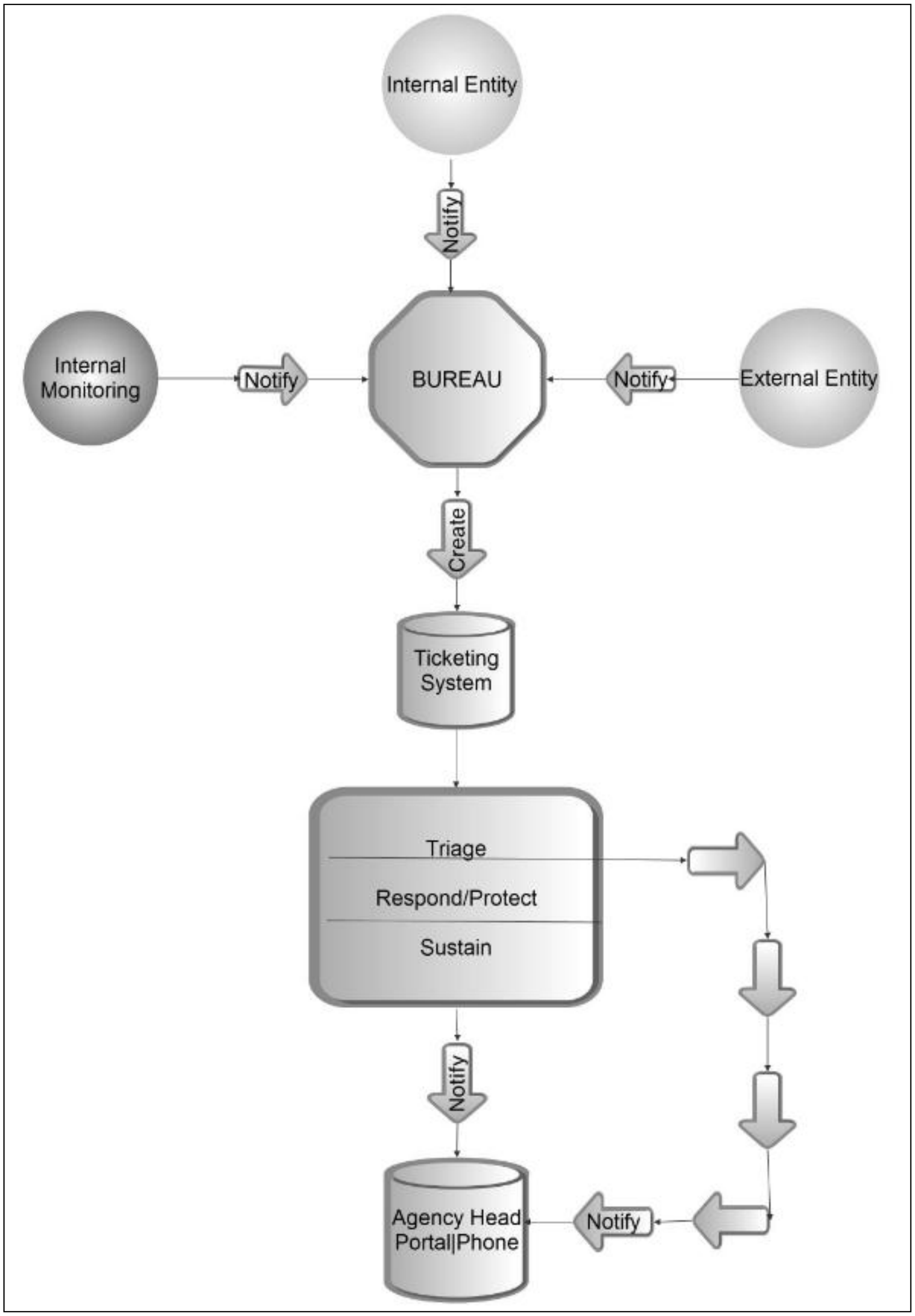
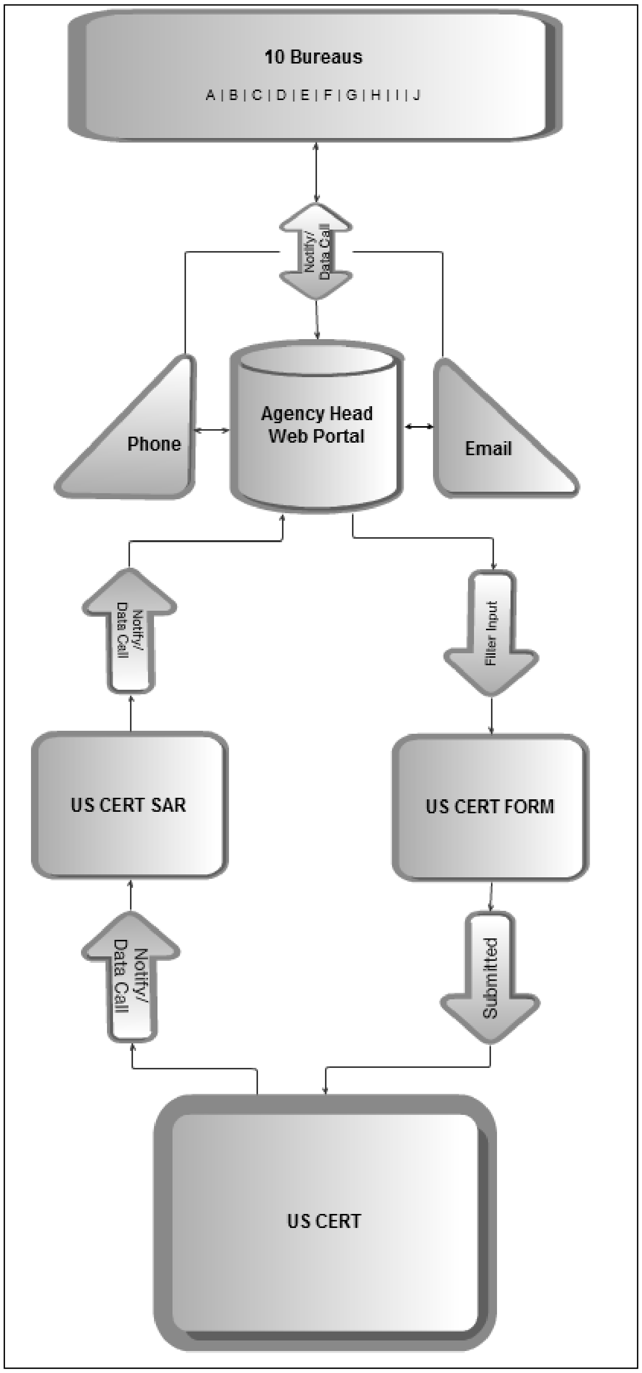


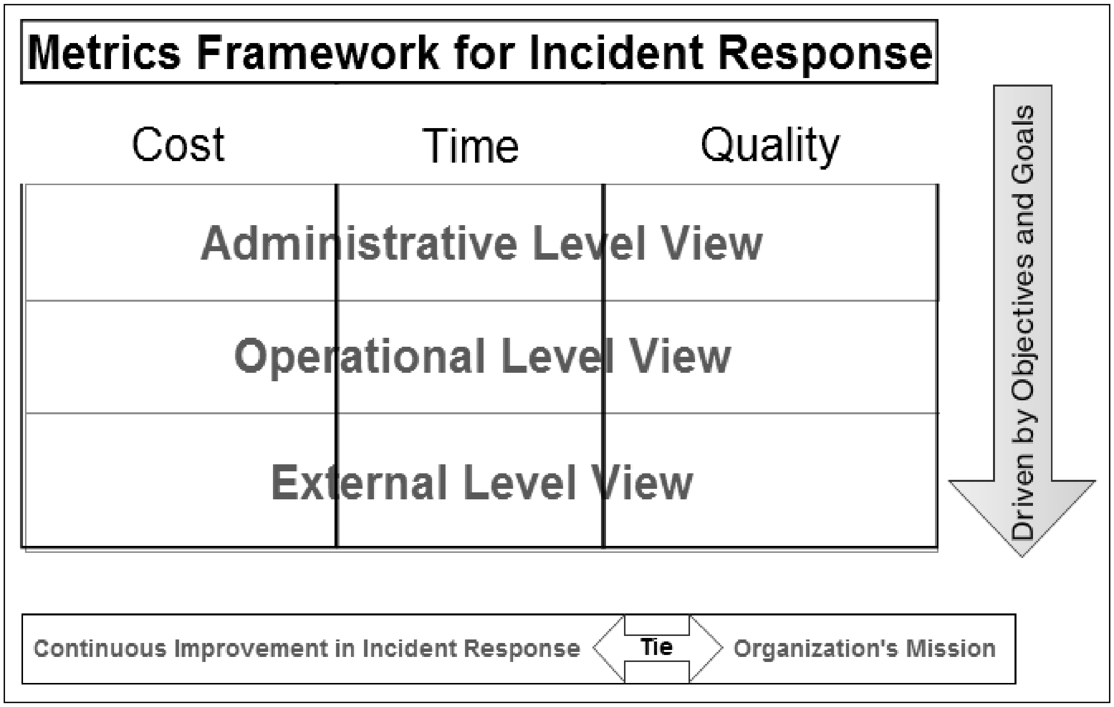
Figure 7: Agency Level Process Flow.



To identify the process flow for CSIR capabilities it is important to identify information assets and stakeholders within a CSIRT. Aside from looking at an inventory list it is best to look at policies and guides produced by CSIRTs. Usually the policies will outline current capabilities and processes with a bureau's CSIRT. However, not all organizations follow their existing policies and guides. Therefore, it is best to verify known process flows. An effective way to determine process flows is through discussion with CSIRTs and directors of CSIRTs. This can be invaluable in identifying process flows for CSIR capabilities.

Over time the amount of known processes and entities involved with CSIR capabilities will accumulate. With more accurate information process flow, identification can help determine the cost and time allotted to each entity within CSIR capabilities. Therefore, process flow identification is crucial to security metrics and offers an illustrated approach towards understanding an organization's CSIR capabilities.

Figure 8: The Metrics Framework for Incident Response.


Metrics Framework for Incident Response
Cost
Time
Quality
Administrative Level View
Operational Level View
External Level View
Driven by Objectives and Goals
Continuous Improvement in Incident Response
Tie
Organization's Mission

As shown in Figure 8, the metrics framework for CSIR includes three types of measurements for CSIR, cost, time, and quality. It identifies the need for objective driven measurements, the need to consider audience groups for measurement evaluations and presenting results, the need to tie measurements to the agency's mission, and the importance of process flow identification. The metrics framework for CSIR is also accompanied by a measurement form for CSIR. The measurement form is specifically geared towards utilizing the framework and creating CSIR security metrics. Overall, the metrics framework for CSIR is a product of the education, work experience, and literature research conducted in search for a common platform for measuring CSIR capabilities.

CONCLUSIONS

In this paper, we argued that there was a need for a metrics framework to measure the performance and creating accountability for computer security incident response (CSIR) capabilities. Subsequently, five elements were identified that were critical to the metrics framework for CSIR: 1) understanding the three types of measures, 2) establishing objective driven metrics, 3) produce results based on audience considerations, 4) tie incident response (IR) evaluations to improve IR capabilities that support the organization's mission, and 5) process flow identification for CSIR. We then concluded that there are three types of measurements for measuring CSIR where measurements must be driven by objectives and goals. Consideration of the audience needs to identify CSIRT metrics and results are critical for satisfying the audience. Moreover, tying measurements to the agency's mission is essential to the success of the security measurement, enabling the user to show the value within a CSIR program.

REFERENCES

Alberts, C., Allen, J., & Stoddard, R. (2011). *Security measurement and analysis*, pp. 19-21. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.

Alberts, C., Dorofee, A., Killcrece, G., Ruefle, R., & Zajicek, M. (2004). *Defining incident management process for CSIRTs: A work in progress* [Technical Report CMU/SEI-2004-TR-015 ESC-TR-2004-015], pp. 7-11. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.

Allen, J. H., & Davis, N. (2010). *Measuring operational resilience using the CERT resilience management model [Technical note CMU/SEI-2010-TN-030], pp. 7-15, 23-44.* Software Engineering Institute, Carnegie Mellon University.

Atkinson, R. (1999). Project management: Cost, time, and quality, two best guesses and a phenomenon, its time to accept other success criteria. *International Journal of Project Management, 17*(6), 337-342. Retrieved from http://itee.uq.edu.au/~engg4800/_readings/two%20best%20guesses.pdf

Brewer, P., Garrison, R., & Noreen, E. (2009). *Introduction to managerial accounting (*5th ed.). Columbus, OH: McGraw-Hill/Irwin.

Center for Internet Security Community (CISC). (2010). *The CIS security metrics v.1.1.0*. Retrieved from https://benchmarks.cisecurity.org/tools2/metrics/CIS_Security_ Metrics_ v1.1.0.pdf

Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A., & Robinson, W. (2008). *Performance measurement guide for information security [NIST Special Publication 800-55 Revision 1]*, pp. 12-15, 22-27. Gaithersburg, MD: NIST. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf

Dorofee, A., Killcrece, G., Ruefle, R., & Zajicek, M. (2007). *Incident management capability metrics: Version 0.1*, pp. 4-20. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.

Ellis, J., Fisher, D., Longstaff, T., Pesante, L., & Pethia, R. (1997). *Report to the president's commission on critical infrastructure protection [Special Report CMU/SEI-97-SR-003]*, pp. 19-20. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.

Federal Information Security Management Act of 2002, 44 U.S.C. § 3541. (2002).

Hopkins, E. (2009). *United States Information and Communication Enhancements Act of 2009*. Presentation to the Subcommittee on Federal Financial Management, Government Inforamtion, Federal Services, and International Security. Retrieved from http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2009-04/ispab_ehopkins_ april2009.pdf

Jansen, W. (2009). *Directions in security metrics research [NISTIR 7564] pp.* 10-15. Gaithersburg, MD: NIST. Retrieved from http://csrc.nist.gov/publications/nistir/ir7564/nistir-7564_metrics-research.pdf

Niven, R. P. (2008) *Balanced scorecard: Step-by-step for government and nonprofit agencies*, pp. 15-22. Hoboken, NJ: John Wiley & Sons.

Payne, C. S. (2006) A guide to security metrics, pp. 1-3. [White Paper]. Retrieved from http://www.sans.org/reading_room/whitepapers/auditing/guide-security-metrics_55

Rezmierski, V. E., Deering, S., Fazio, A., & Ziobro, S. (1998). *Incident cost analysis and modeling project: A report from the CIC security working group to the CIC chief information officers*, pp. 13-15. Ann Arbor, MI: University of Michigan.

Scarfone, K., Grance, T., & Masone, K. (2008). *Computer security incident handling guide: Recommendations of the National Institute of Standards and Technology [Special Publication 800-61, Revision 1]*, pp. 2-16, 3-13, 3-14, 3-26. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

Soanes, C., & Stevenson, A. (2008). *Concise Oxford English dictionary*, 12th ed. New York, NY: Oxford University Press.

Top 10 computer viruses. (2010, July). *PC Tools*. Retrieved from http://www.pctools.com/security-news/top-10-computer-viruses/

U. S. Department of Homeland Security, Computer Emergency Readiness Team (CERT). (n.d.). *Federal incident reporting guidelines*. Retrieved from http://www.us-cert.gov/federal/reportingRequirements.html

U. S. Department of Homeland Security, Office of the Inspector General. (2010). DHS needs to improve the security posture of its cybersecurity program systems [OIG-10-111]. Retrieved from http://www.oig.dhs.gov/assets/Mgmt/OIG_10-111_Aug10.pdf

U. S. Government Accountability Office (GAO). (2010). *Cybersecurity: Progress made but challenges remain in defining and coordinating the comprehensive national initiative*.

General Accounability Office, United States, GAO-10-338. Retrieved from http://www.gao.gov/new.items/d10338.pdf

West-Brown, M. J., Stikvoort, D., Kossakowski, K. –P., Killcrece, G., Ruefle, R., & Zajicek, M. (2003). Handbook for computer security incident response teams (CSIRTs) 2nd ed. [CMU/SEI-2003-HB-002], pp. 10-11, 40-55, 191. Pittsburgh, PA: *Software Engineering Institute, Carnegie Mellon University*. Retrieved from http://www.cert.org/archive/pdf/csirt-handbook.pdf

The White House. (2009). Cyberspace policy review: Assuring a trusted and resilient information and communications infrastructure, pp. 1-5. Retrieved from http://www.whitehouse. gov/assets/documents/Cyberspace_Policy_Review_final.pdf

The White House, Office of Management and Budget (OMB). (n.d.). Appendix III to OBM circular no. A-130. Retrieved from http://www.whitehouse.gov/omb/circulars_a130_a130appendix_iii

Wilshusen, C. G. (2011). Cybersecurity: Continued attention needed to protect our nation's critical infrastructure and federal information systems: *Testimony before the subcommittee on cybersecurity, infrastructure protection and security technologies, committee on homeland security, House of Representatives* [GAO-11-463T]. Retrieved from http://www.gao.gov/new.items/d11463t.pdf

Xie, N., & Mead, R. N. (2004). *SQUARE Project: Cost/benefit analysis framework for information security improvement projects in small companies*, pp. 4-22. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University. Retrieved from www.cert.org/archive/pdf/SQUARE_Cost.pdf

APPENDIX A: DEFINITION OF TERMS

Computer Security Incident Response Team: "an organization or team that provides services and support to a defined constituency for preventing, handling, and responding to computer security incidents" (Alberts et al., 2004).

Framework: "an essential supporting or underlying structure" (Soanes & Stevenson, 2008).

Incident: "any event that takes place through, on, or constituting information technology resources that requires a staff member or administrator to investigate and/or take action to reestablish, maintain, or protect the resources, services, or data of the community or individual members of the community" (Rezmierski et al., 1998).

Measurement: "single-point-in-time views of specific, discrete, factors" (Payne, 2006).

Metric: "generated from analysis; derived by comparing to a predetermined baseline two or more measurements taken over time" (Payne, 2006).

Triage: "The process of receiving, initial sorting, and prioritizing of information to facilitate its appropriate handling" (West-Brown et al., 2003).

Personally Identifiable Information (PII): "any information about an individual that is maintained by an agency, including information that can be used to distinguish or trace an individual's identity, such as name, Social Security Number, date and place of birth, mother's maiden name, biometric records, and any other personally information that is linked or linkable to an individual" (U. S. General Accountability Office, 2008).

APPENDIX B: FORMULAS FOR COMPUTER SECURITY INCIDENT RESPONSE BY CENTER FOR INTERNET SECURITY*

$$\mathrm{COI} = \sum(\text{Direct Loss} + \text{Cost of Business System Downtime} + \text{Cost of Containment} + \text{Cost of Recovery} + \text{Cost of Restitution})$$

Cost of Incidents

$$MCOI = \frac{\sum\begin{gathered}(Direct\_Loss + Cost\_Business\_Downtime + \\ Cost\_Containment + Cost\_Recovery + Cost\_Restitution)\end{gathered}}{Count(Incidents)}$$

Mean Cost of Incidents

$$MIRC = \frac{\sum(Cost\_Recovery)}{Count(Incidents)}$$

Mean Cost of Incident Recovery

$$MTTID = \frac{\sum(Date\_of\_Discovery - Date\_of\_Occurrence)}{Count(Incidents)}$$

Mean Time to Incident Discovery

$$MTBSI = \frac{\sum(Date\_of\_Occurence[Incident_{n}] - Date\_of\_Occurence[Incident_{n-1}])}{Count(Incidents)}$$

Mean Time between Security Incidents

$$MTIR = \frac{\sum(Date\_of\_Recovery - Date\_of\_Occurrence)}{Count(Incidents)}$$

Mean Time to Incident Response

***All Formulas are in the public domain and were developed by the Center for Internet Security (CISC, 2010).**

APPENDIX C: ACRONYMS

ACISO	Association Chief Information Security Officer
CERT/CC	Computer Emergency Response Team Coordination Center
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMU	Carnegie Mellon University
CSIR	Computer Security Incident Response
CSIRC	Computer Security Incident Response Center
CSIRT	Computer Security Incident Response Team
DARPA	Defense Advanced Research Project Agency
DHS	Department of Homeland Security
FISMA	Federal Information Security Management Act
FIRST	Forum on Incident Response and Security Teams
ID	Identification
IDS	Intrusion Detection System
IG	Inspector General
IR	Incident Response
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PII	Personally Identifiable Information
SEI	Software Engineering Institute Team

This Page Was Left Blank Intentionally.