Use Case for Measuring US-CERT Timeframe Reporting: Applying 5 Critical Elements for Developing a Metrics Framework in Computer Security Incident Response

Vincent Sritapan
Walter Stewart
Jake Zhu
C. E. Tapie Rohm Jr.
California State University San Bernardino

ABSTRACT

Computer security incident response (CSIR) is designed to support Departments and Agencies (DAs) mission by protecting, detecting, triaging, and responding to incidents as they occur. Within the United States Federal Government, DAs are required by the Federal Information Security Management Act of 2002 and by the Office of Management and Budget Circular No. A-120, Appendix III to maintain incident response capabilities. To protect DAs' mission, incident response (IR) capabilities must continually improve to better respond to the advancements of cyber threats. Measuring the efficiency and effectiveness of a CSIR program becomes an essential function for maintaining the overall security state of DAs. The challenge lies in applying security metrics to a CSIR program to improve IR. To address this concern and support CSIR efforts, a use case is demonstrated through the application of five critical elements for developing a metrics framework within CSIR. The goal is to provide a holistic approach towards security metrics, which is specific to incident reporting and promotes efforts for practical, clear, and reusable metrics when measuring a CSIR program.

INTRODUCTION

Incident response is the action taken by Departments and Agencies (DAs) after a "violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices" (Scarfone, Grance, & Masone, 2008). These actions to protect, detect, triage, and respond to incidents (Alberts, Dorofee, Killcrece, Ruefle, & Zajicek, 2004) fulfill requirements as specified by the Office of Management and Budget (OMB). DAs must "ensure that there is a capability to provide help to users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats" (OMB Circular No. A-130, Appendix III). To measure the efficiency and effectiveness of CSIR capabilities we apply five critical elements for developing a metrics framework within CSIR; These five critical elements include 1) understanding the three types of measures, 2) establishing objective driven metrics, 3) produce results based on audience considerations, 4) tie IR evaluations to improve IR capabilities that support the organization's mission, and 5) process flow identification for CSIR (Sritapan, Stewart, Zhu, & Rohm, 2011). By applying these five critical elements for developing a metrics framework within CSIR, this use case will demonstrate a technology agnostic approach helping to improve IR capabilities and the overall security state of DAs. It is specifically applied to the United States federal government and is intended to help middle management develop and apply a metrics framework for CSIR to improve their IR capabilities.

LITERATURE REVIEW

Since the early 1990s, from the Defense Advanced Research Project Agency's push for Carnegie Melons' Computer Emergency Response Team Coordination Center to the establishment of United States Computer Emergency Readiness Team (US-CERT) by the Department of Homeland Security (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 (H.R. 2458—56), OMB directives (OMB Circular No. A-130, Appendix III), and Inspector General (IG) audits (Department of Homeland Security, 2010). However, the effectiveness for measuring performance and compliance still remains a controversy (General Accountability Officer, 2010; Hopkins, 2009). Audits have continually evolved from yes and no questions to how many and why (Gorsen, Personal Communication, 2010). Efforts to effectively account for programs such as CSIR have become an area of concern.

Currently, United States federal agencies repeatedly report an increased number of security incidents (General Accountability Office, 2011), including a 650% increase in 5 the past years (Chabrow, 2011). Efforts to standardize and sanitize incidents for the purpose of sharing knowledge are currently being applied (Verizon, 2010). New working groups regarding CSIR, such as the Managed Incident Lightweight Exchange, are being proposed to improve information sharing based on the incident handling process (The Internet Engineering Task Force, 2011). The current developments demonstrate efforts to effectively account for CSIR and share information for the benefit of CSIR as a whole.

Measurement framework for computer security incident response

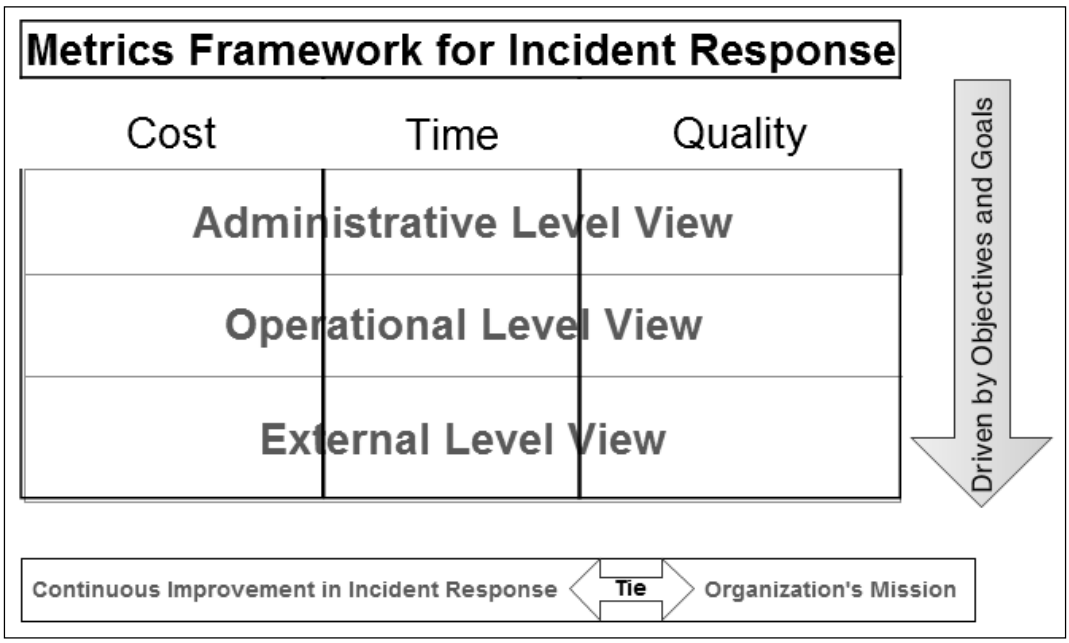


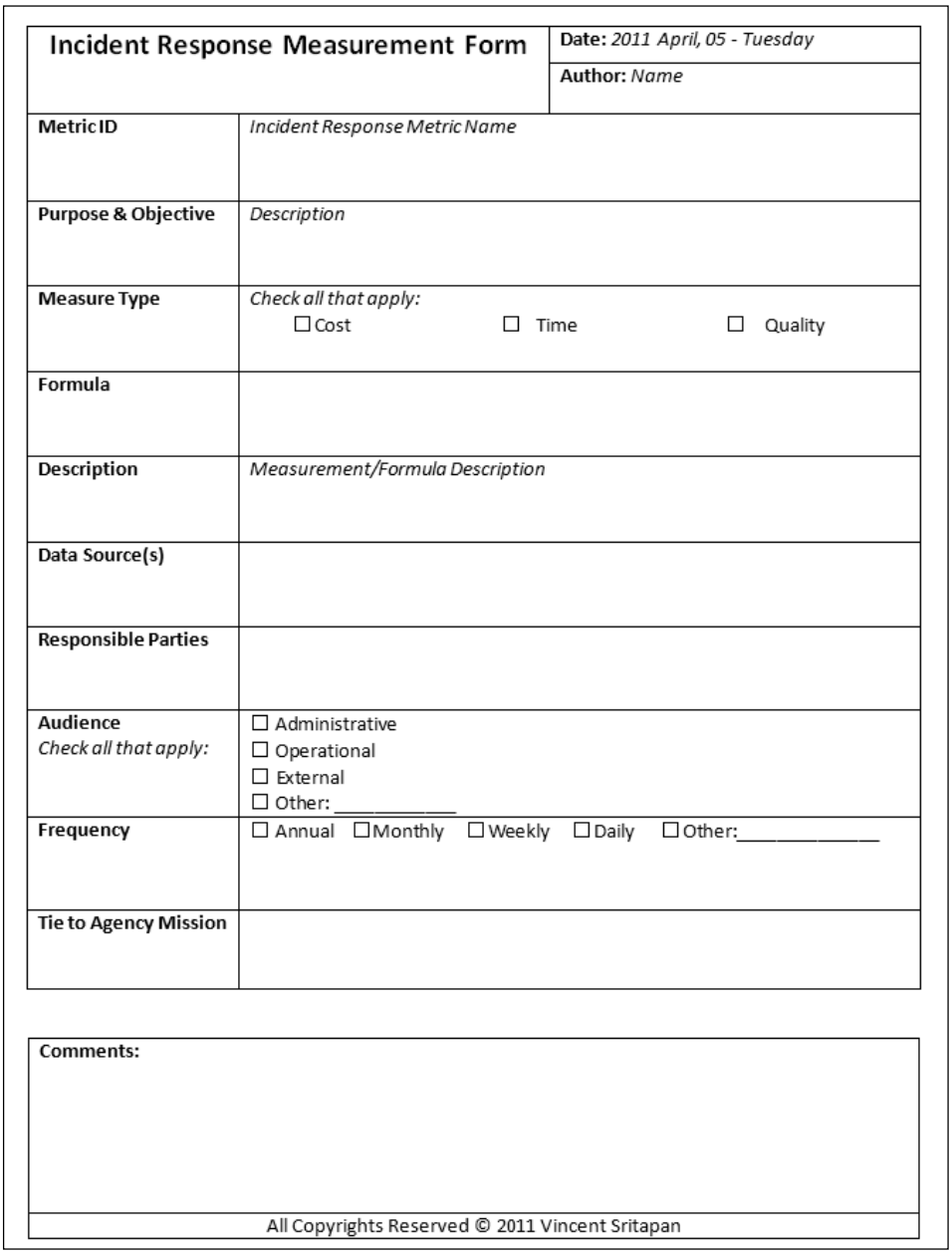
Figure 1. Metrics Framework for Incident Response

The application of this use case draws from five critical elements for developing a metrics framework for CSIR. As shown in Figure 1 above, the metrics framework for CSIR (Sritapan, Stewart, Zhu, & Rohm, 2011) includes three types of measurements, cost, time, and quality. This first critical element presents a holistic and technology agnostic approach for analyzing incidents because it offers the ability to view all types of metrics found within an incident report. The second critical element identifies the need for

objective driven measurements, meaning all measurements have a clear purpose and reason for measuring. The third critical element includes the need to consider audience groups for measurement evaluations and presenting results. This aspect applies the knowledge of knowing who your audience is and how to appropriately capture measurements that meets the need of the intended audience. The fourth critical element is tying measurements to DAs mission. This is specifically important because it allows others to understand how measuring IR ties into supporting the mission of DAs. Lastly, the fifth critical element specific to applying the metrics framework is process flow identification. This element continues to identify more components within the incident response process as the investigation to outline and understand the incident response process becomes apparent (Sritapan, Stewart, Zhu, & Rohm, 2011). Throughout this use case the application of these five critical elements for developing a metrics framework for CSIR will be used.

PREPARATION: MEASUREMENT FORM FOR CSIR

To start off the application of the metrics framework for CSIR we have prepared a measurement form for CSIR. The measurement form is specifically geared towards utilizing the framework and creating CSIR security metrics. To prepare for this use case the development of a Incident Response Measurement Form is needed. The Incident Response Measurement Form shown below draws from National Institute of Standards and Technology (NIST) Special Publication 800-55 Measure 10 and Center for Internet Security (CIS) Security Metrics v1.1.0 (See Figure 2. Incident Response Measurement Form Part 1, Below). The names and definitions for each section differ from existing documentation, so please be sure to read the following descriptions.



Incident Response Measurement Form	Date: *2011 April, 05 - Tuesday* Author: *Name*
Metric ID	*Incident Response Metric Name*
Purpose & Objective	*Description*
Measure Type	*Check all that apply:* ☐ Cost ☐ Time ☐ Quality
Formula	
Description	*Measurement/Formula Description*
Data Source(s)	
Responsible Parties	
Audience *Check all that apply:*	☐ Administrative ☐ Operational ☐ External ☐ Other: _____
Frequency	☐ Annual ☐ Monthly ☐ Weekly ☐ Daily ☐ Other:_____
Tie to Agency Mission	

Comments:

Figure 2. Incident Response Measurement Form Part 1

"Metric ID" is a number and/or letter that is assigned by the person conducting the measurement. Following the Metric ID is the metric name, also given by the person conducting the measure. "Purpose & Objective" is the section where the purpose and objective of the measurement is stated. This is stated before the actual measurement formula and is essential to creating a meaningful measurement.

"Measurement Type" is a section with three check boxes that allows the user of the form to choose which of the three types of measures are being conducted. Please note that the measurement can involve one to as many as three measurement types in the measurement form.

“Formula” is the section where the formula for the measurement can be outlined and detailed. This is a critical part of the measurement because it enables for others to understand how the measurement is being conducted. Using formulas enables others to repeat the measurement and use it for their own measurement purposes.

“Description” is the section that clarifies the meaning of the formula. If there are any exceptions, notations, etc. the author of the form can explain the formula in detail.

“Data Source(s)” is the section where assets containing or controlling sources of data for the measurement are identified. Depending on the agency this can involve one or many sources of data.

“Responsible Parties” is the section that identifies who is responsible for conducting and overseeing the measurement. This could involve technicians, analysts, and/or upper management.

“Audience” is a section that identifies the intended audience. This may comprise of one or multiple viewing audiences depending on the situation.

“Frequency” is the mode of measurement. It is a selection for periods of time for when the measurement is to be conducted or what points of time they wish to review.

“Tie to Agency Mission” is a section that tries to put into words how the measurement ties into the agency’s mission.

“Comments” is a free section for the author/user to use this form and place any notes or comments necessary for the measurement. The Comment section is a space that is utilized at the user’s discretion.

Revision History

Date	Notes	Name

Figure 3. Incident Response Measurement Form Part 2

Security metrics in CSIR should be controlled and collected for reuse, so that knowledge gained from FISMA and other audits can be addressed for future purposes. An additional aspect for the measurement form is the revision control history form that is attached to each metric (See Figure 3. Incident Response Measurement Form Part 2, Above). The above form is intended for CSIRTs and CSIR stakeholders to reuse the metric ID and formula. Aside from creating a practical and clear guide for security metrics regarding CSIR, this use case also looks to promote collaborations supporting the archiving of security metrics for future use.

USE CASE SCENARIO

In this scenario, an agency containing 10 bureaus is making preparations at the headquarter level for a FISMA audit under the program of incident management. One of the anticipated questions is the compliance for timeframe reporting. The samples of incidents for the 10 bureaus, Bureaus A through J, are shown in Table 1. Sample Incident Reports. For simplification only category 1, unauthorized access, 2, denial of service, and 3, malicious code, incidents were used in this case (See Appendix C United States Computer Emergency Readiness Team Reporting Criteria for incident categories). Note that federal agency must adhere to US-CERT timeframe reporting requirements (US-CERT, 2011).

The case scenario is an audit preparation that involves security measurements for timeframe reporting and it illustrate the use of the metrics framework for CSIR. Please refer to Appendix A for federal agency incident criteria and timeframe reporting requirements.

Before providing the sample data, it is important to understand that each CSIRT will have their own incident reports for measuring depending on their agency's CSIR capabilities. Some agencies may have more or less data points to measure depending on the maturity of their CSIR program. Also, as noted in the assumptions in Chapter One, the agency must have CSIR capabilities and must collect data points for measuring CSIR capabilities. The data points can usually be found at the CSIR Center or with the CSIRT. CSIRTs should have the necessary data specific to measuring timeframe reporting.

Before looking at the sample data, Figure 10. Columns and Names for Sample Incident Reports describes each column respective to their column title. The format of the data for each column is shown in Figure 11. Columns and Names for Sample Incident Reports and described in the following paragraph.

Ticket No.	Bureau	Category	Subject	Occurred	Reported	Created	Submit US-CERT	Type	PII	Status
####	Letter	0-6	Text	YYYY.MM.DD.HH.MM.SS	YYYY.MM.DD.HH.MM.SS	YYYY.MM.DD.HH.MM.SS	YYYY.MM.DD.HH.MM.SS	Cyber/ Equipment/ Physical	Yes/ No	Open/ Closed

Figure 4. Columns and Names for Sample Incident Reports

As shown in Figure 4. Columns and Names for Sample Incident Reports, "Ticket No." refers to the assigned number when an incident is reported to the agency headquarters level. "Bureau" letter is the bureau letter, similar to a bureau name that would represent the bureau. "Category" is the incident type as defined by US-CERT and NIST Special Publication 800-61. Notably, an incident can have more than one assigned category. "Subject" text is the subject name for the incident, which can also include a limited text description. "Occurred" is the estimated time of an incident occurrence. This can sometimes be exact if the data capture is electronic, but it is normally a perceived time that an individual determines. "Reported" is the time an incident is first reported at the bureau level. "Created" displays the time the incident is reported/submitted from the bureau CSIRT to the agency headquarter CSIRT. "Submit US-CERT" displays the time the incident is submitted from the agency headquarters CSIRT to US-CERT. Please note that the time is constructed with the year, month, day, hour, minute, and second. "Type" is the type of incident in regards to a physical paper incident, equipment incident, or cyber incident. "PII" is the column that identifies if the incident involves personally identifiable information (PII). "Status" is in regards to whether an incident ticket no. is still open or if it has been closed.

SAMPLE DATA

According to the scenario, the sample incident reports came from the CSIRT at the agency headquarters level. The information from the sample incident reports is being used to measure performance on CSIR timeframe reporting. This is in preparation for the upcoming FISMA audit. The data set for this scenario can be found in Table 1. Sample Incident Reports below.

Table 1. Sample Incident Reports

Ticket No./	Bureau	Category/	Subject	Occurred	Reported	Created	Submit US-CERT	Type	PII	Status
1	A	1	N/A	2011.01.01.14.00.00	2011.01.01.14.45.11	2011.01.01.15.05.15	2011.01.01.15.15.16	Cyber	Yes	Closed
2	B	2	N/A	2011.01.01.16.30.00	2011.01.02.08.45.45	2011.01.02.10.15.23	2011.01.02.10.25.24	Cyber	No	Closed
3	C	1	N/A	2011.01.01.18.00.00	2011.01.02.10.28.13	2011.01.02.11.08.14	2011.01.02.11.18.15	Phys	Yes	Closed
4	D	1	N/A	2011.01.02.08.15.00	2011.01.03.11.40.26	2011.01.03.11.55.27	2011.01.03.12.05.28	Cyber	Yes	Closed
5	E	3	N/A	2011.01.02.14.00.00	2011.01.03.14.45.27	2011.01.03.19.45.28	2011.01.03.19.54.29	Equip	No	Open
6	F	1	N/A	2011.01.03.12.00.00	2011.01.04.04.40.28	2011.01.04.05.33.29	2011.01.04.05.42.30	Phys	Yes	Closed
7	G	3	N/A	2011.01.05.04.45.00	2011.01.06.08.10.29	2011.01.06.16.10.30	2011.01.06.16.19.31	Cyber	No	Closed
8	H	1	N/A	2011.01.06.11.00.00	2011.01.08.14.22.30	2011.01.08.14.52.11	2011.01.08.15.01.12	Cyber	Yes	Closed
9	I	1	N/A	2011.01.06.14.30.00	2011.01.09.20.16.31	2011.01.10.20.16.32	2011.01.10.21.24.33	Equip	No	Open
10	J	1	N/A	2011.01.11.14.00.00	2011.01.12.14.12.12	2011.01.12.14.12.12	2011.01.12.14.20.13	Phys	Yes	Closed
11	A	2	N/A	2011.01.11.16.45.00	2011.01.18.07.40.31	2011.01.18.08.30.22	2011.01.18.08.38.23	Cyber	No	Closed
12	B	3	N/A	2011.02.01.11.15.00	2011.02.12.05.45.55	2011.02.14.11.45.56	2011.02.14.11.53.57	Phys	No	Closed
13	B	1	N/A	2011.02.07.08.15.00	2011.02.13.07.38.25	2011.02.13.08.28.00	2011.02.13.08.36.01	Equip	Yes	Open
14	C	3	N/A	2011.02.17.19.30.00	2011.02.19.17.20.36	2011.02.20.11.20.37	2011.02.20.11.30.38	Cyber	No	Closed
15	D	2	N/A	2011.02.11.07.00.00	2011.02.23.19.22.22	2011.02.23.20.12.23	2011.02.23.20.21.24	Phys	No	Closed
16	D	1	N/A	2011.02.21.12.00.00	2011.02.24.14.40.38	2011.02.24.20.20.19	2011.02.24.20.29.20	Cyber	Yes	Closed
17	E	1	N/A	2011.01.07.19.30.00	2011.02.24.18.49.26	2011.02.24.18.59.11	2011.02.24.19.08.12	Cyber	Yes	Closed
18	F	2	N/A	2011.01.16.18.15.00	2011.02.27.23.40.40	2011.02.28.08.05.41	2011.02.28.08.14.42	Phys	No	Closed
19	F	2	N/A	2011.03.01.05.45.00	2011.03.02.21.28.19	2011.03.03.11.28.20	2011.03.03.11.38.21	Phys	No	Closed
20	G	1	N/A	2011.01.21.04.45.00	2011.03.07.15.41.42	2011.03.07.16.11.43	2011.03.07.16.19.44	Cyber	Yes	Closed
21	H	2	N/A	2011.02.11.14.00.00	2011.03.10.19.10.33	2011.03.11.09.11.22	2011.03.11.09.20.23	Cyber	No	Closed
22	H	2	N/A	2011.01.09.22.15.00	2011.03.12.16.09.44	2011.03.12.17.09.45	2011.03.12.17.19.46	Cyber	No	Closed
23	I	1	N/A	2011.03.01.21.30.00	2011.03.15.19.33.52	2011.03.16.08.55.53	2011.03.16.10.03.54	Equip	Yes	Open
24	J	3	N/A	2011.02.11.09.45.00	2011.03.18.23.30.41	2011.03.18.23.30.41	2011.03.18.23.39.42	Cyber	No	Closed
25	J	1	N/A	2011.03.01.22.15.00	2011.03.19.09.43.37	2011.03.19.09.43.37	2011.03.19.09.52.38	Phys	Yes	Closed

METRIC DEVELOPMENT

For the analysis of this case scenario, Metric ID 001, 002, and 003 were created (See Figure 5. Measurement Form for Metric ID 001, Figure 6. Measurement Form for Metric ID 002, Figure 7. Measurement Form for Metric ID 003, below). Metric ID 001 looks at the number of incidents for the agency based on incident categories 0 through 6. Metric ID 002 looks at the duration for each incident against the time required to report. Metric ID 003 looks at the percentage of incidents reported on time. The analysis identifies the current status of the CSIR capabilities as well as usage of the metrics framework.

STEP BY STEP APPLICATION

Using the metrics framework, the measurement form is applied for each metric developed. First, the objective and purpose is clearly stated. Second, the type of measurement is identified. Third, the formula and description is detailed. Fourth, the data sources and responsible parties are identified. Fifth, the audience group is selected. Sixth, the frequency of the sample or measurement is determined. Seventh, the statement for tying the measurement to the organization's mission is stated. Eighth, the comments are filled in. Then, after the first metric is developed, more metrics may be developed if needed. Finally, the measurement is conducted and the results are analyzed. Depending on the findings, action may be taken

to improve CSIR capabilities. In the case scenario each metric developed will be described, following this step by step application. The decisions to be made will be identified and resolution will be stated.

Incident Response Measurement Form	**Date:** *2011 April, 05 – Tuesday* **Author:** Vincent Sritapan
Metric ID 001	Number of Incidents for Category 0 – 6
Purpose & Objective	Prepare for FISMA Audit Determine number of incidents
Measure Type	*Check all that apply:* ☐ Cost ☐ Time ☒ Quality
Formula	Incident Count by Category = Count (Category # Incidents) Total Incidents for Agency = ∑ Count (Category 0 - 6 Incidents)
Description	Incident count by category is the number incidents separated by category type. Total Incidents for Agency includes all reported incidents for the Agency for a defined period of time.
Data Source(s)	Agency CSIRC Bureau CSIRTs (A through J)
Responsible Parties	Agency 1 Headquarters, Division 1 Program Manager: Name ABC Contract Analyst Group: Senior Analyst, Junior Analyst
Audience *Check all that apply:*	☒ Administrative ☐ Operational ☐ External ☐ Other: _____
Frequency	☐ Annual ☐ Monthly ☐ Weekly ☐ Daily ☒ Other: FISMA YEAR
Tie to Agency Mission	Helps organization understand the volume of incidents being reported Intended for FISMA Audit by DHS.

Comments:

Step 1: Determine what incidents are being reported.
Metric ID 001, 002, 003, 004 All grouped for FISMA Audit in Incident Management.

Figure 5. Measurement Form for Metric ID 001

Metric ID 001 is shown in the Figure 11. Measurement Form for Metric ID 001 above and is a quality measurement type that documents at incident counts by category and total incidents for the agency. The purpose and objective for the measurement is to prepare for the upcoming FISMA audit and determine the number of incidents that have occurred for the agency. The data source is the agency CSIR center (CSIRC) as well as the bureau CSIRT. The responsible parties include the agency program manager and the contracting team. The frequency is selected as “other” to include the FISMA year. This scenario is

defined as January 1st, 2011 through May 1st, 2011. This metric is tied to the agency's mission since it helps determine the volume of incidents reported that are relevant for the FISMA audit. The comments section shows that this metric is the first step for preparing for the upcoming FISMA audit and that metric ID 002, 003, and 004 are all related.

Incident Response Measurement Form	**Date:** *2011 April, 05 - Tuesday* **Author:** Vincent Sritapan
Metric ID 002	Duration for Category 0-6 Incidents
Purpose & Objective	Preparations for FISMA Audits Determine if Agency 1 is compliant for reporting incidents
Measure Type	*Check all that apply:* ☐ Cost ☒ Time ☐ Quality
Formula	Duration (*Time Created to Time Submitted to US-CERT*) less *Time Required*
Description	Time Created is the first official notification time to Agency HQ Time Submitted to US-CERT is the end time for required timeframe reporting Time Required depends on Category 0-6 (Please see US-CERT.gov)
Data Source(s)	Agency CSIRC Bureau CSIRTs (A through J)
Responsible Parties	Agency 1 Headquarters, Division 1 Program Manager: Name ABC Contract Analyst Group: Senior Analyst, Junior Analyst
Audience *Check all that apply:*	☒ Administrative ☐ Operational ☒ External ☐ Other: _____
Frequency	☐ Annual ☐ Monthly ☐ Weekly ☐ Daily ☒ Other: FISMA YEAR
Tie to Agency Mission	Helps organization meet timeframe reporting compliance. Intended for FISMA Audit by DHS.

Comments:

Step 2: Determine Duration of Incident Reports
Metric ID 001, 002, 003, 004 All grouped for FISMA Audit in Incident Management.

Figure 6. Measurement Form for Metric ID 002

Metric ID 002 is shown in Figure 6. Measurement Form for Metric ID 002 above is a time measurement type that determines the duration of an incident and the time required to report. The purpose and objective for the measurement is to prepare for the coming FISMA audit and determine that the agency is compliant

in its timeframe reporting. The data source is the agency CSIR center (CSIRC) as well as the bureau CSIRT. The responsible parties include the agency program manager and contracting team. The frequency is selected as "other" to include the FISMA year. This metric is tied to the agency's mission because it helps determine if the agency is meeting the timeframe reporting requirements. The comments section shows that this metric is the second step for preparing for the upcoming FISMA audit and that metric ID 002, 003, and 004 are all related.

Incident Response Measurement Form	**Date:** *2011 April, 05 - Tuesday* **Author:** Vincent Sritapan
Metric ID 003	Percentage of Incidents Reported on Time
Purpose & Objective	Preparations for FISMA Audits Determine if Agency 1 is compliant for reporting incidents
Measure Type	*Check all that apply:* ☐ Cost ☒ Time ☒ Quality
Formula	% of Incidents Reported on Time = Number of Incident Reported on Time / Total Number of Incidents Reported
Description	Percentage of incidents reported on time is determined by the category type. (Please see US-CERT.gov)
Data Source(s)	Agency CSIRC Bureau CSIRTs (A through J)
Responsible Parties	Agency 1 Headquarters, Division 1 Program Manager: Name ABC Contract Analyst Group: Senior Analyst, Junior Analyst
Audience *Check all that apply:*	☒ Administrative ☐ Operational ☒ External ☐ Other: _____
Frequency	☐ Annual ☐ Monthly ☐ Weekly ☐ Daily ☒ Other: FISMA YEAR
Tie to Agency Mission	Helps organization meet timeframe reporting compliance. Intended for FISMA Audit by DHS.

Comments:

Step 3: Determine Compliance Percentage
Note: Management wants 95% and above on time reporting.
*All Incidents not reported on time must have documentation.
Metric ID 001, 002, 003, 004 All grouped for FISMA Audit in Incident Management.

Figure 7. Measurement Form for Metric ID 003

Metric ID 003 is shown in Figure 7. Measurement Form for Metric ID 003 above and is a time and quality measurement type that determines the percentage of incidents reported on time. The purpose and

objective for the measurement is to prepare for the upcoming FISMA audit and determine if the agency is compliant in its timeframe reporting. The data source is the agency CSIR center (CSIRC) as well as the bureau CSIRT. The responsible parties include the agency program manager and contracting team. The frequency is selected as other to include the FISMA year. This metric is tied to the agency's mission because it helps determine if the agency is meeting their timeframe reporting requirements. The comments section shows that this metric is the third step for preparing for the upcoming FISMA audit and that management requires 95% compliance for incidents reported on time.

SCOPE OF ANALYSIS

The analysis shows that there are 25 incidents reported for the agency. For this case scenario the agency headquarters CSIRT was asked to prepare for the FISMA audit based on compliance for timeframe reporting. The only points of time that are of interest to the audit are the "Created" and "Submit US-CERT" times. At the agency headquarters level the time to report begins once the incident is reported. Using the given data set the "Created" is the time reported at the agency headquarters CSIRT level. With the given information all incidents regarding PII are required to be reported in one hour of notification. The scope of the analysis and its results are taken from the agency headquarters point of view.

RESULT

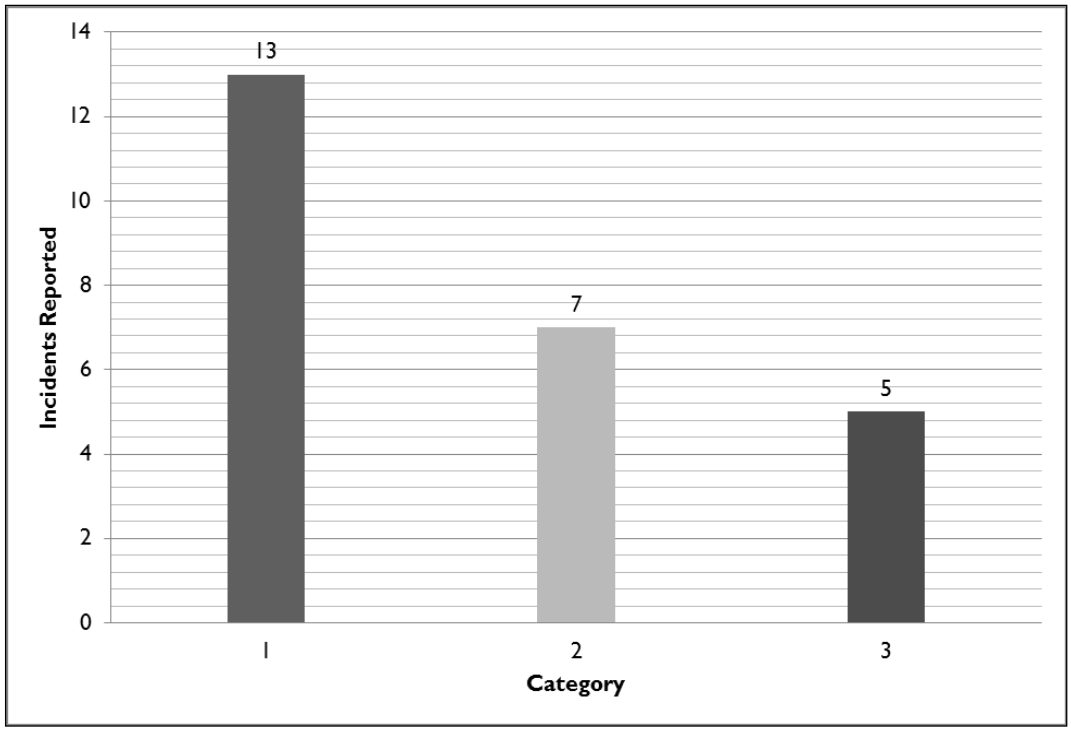


Figure 8. Incident Count by Category

For Metric ID 001 we find that there are a total of 25 incidents reported within the current FISMA year. Of those 25 incidents reported there are 13 category 1 incidents, 7 category 2 incidents, and 5 category 3 incidents (See Figure 8. Incident Count by Category, Above). Additionally, we can illustrate the results by bureau letter in Figure 9. Incident Count by Category and Bureau below.

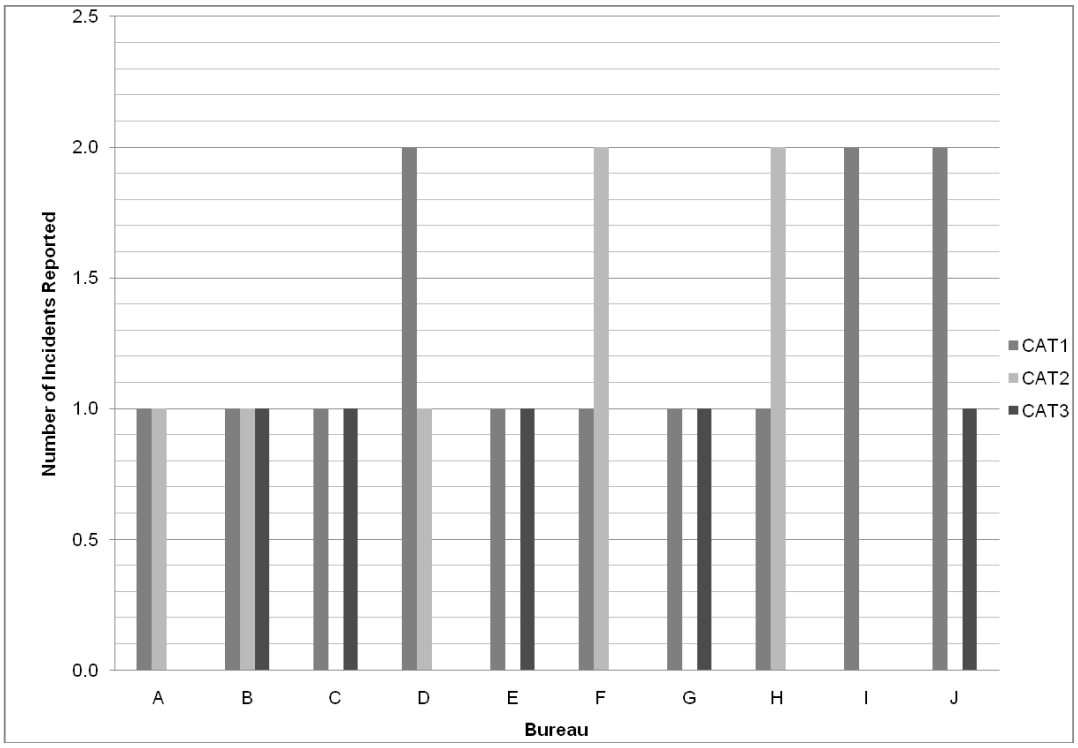


Figure 9. Incident Count by Category and Bureau

For Metric ID 002 we can see that the average time it takes for an incident to be reported from the agency headquarters CSIRT to US-CERT is about 9 minutes with the exception of 2 outliers. The outliers are Ticket No. 10 and 23 involving bureau I and PII for the incidents. Therefore, with the requirement being under one hour, 23 of the 25 incidents have been reported on time.

Table 2. Duration for Sample Incident Reports

Ticket No/ Bureau		Cat.	Created	Submit US-CERT	Duration	Within 1 hour
1	A	1	2011.01.01.15.05.15	2011.01.01.15.15.16	10 min	Yes
2	B	2	2011.01.02.10.15.23	2011.01.02.10.25.24	10 min	Yes
3	C	1	2011.01.02.11.08.14	2011.01.02.11.18.15	10 min	Yes
4	D	1	2011.01.03.11.55.27	2011.01.03.12.05.28	10 min	Yes
5	E	3	2011.01.03.19.45.28	2011.01.03.19.54.29	9 min	Yes
6	F	1	2011.01.04.05.33.29	2011.01.04.05.42.30	9 min	Yes
7	G	3	2011.01.06.16.10.30	2011.01.06.16.19.31	9 min	Yes
8	H	1	2011.01.08.14.52.11	2011.01.08.15.01.12	9 min	Yes
9	I	1	2011.01.10.20.16.32	2011.01.10.21.24.33	1 hour 8 min	No
10	J	1	2011.01.12.14.12.12	2011.01.12.14.20.13	8 min	Yes
11	A	2	2011.01.18.08.30.22	2011.01.18.08.38.23	8 min	Yes
12	B	3	2011.02.14.11.45.56	2011.02.14.11.53.57	8 min	Yes
13	B	1	2011.02.13.08.28.00	2011.02.13.08.36.01	8 min	Yes
14	C	3	2011.02.20.11.20.37	2011.02.20.11.30.38	10 min	Yes
15	D	2	2011.02.23.20.12.23	2011.02.23.20.21.24	9 min	Yes
16	D	1	2011.02.24.20.20.19	2011.02.24.20.29.20	9 min	Yes
17	E	1	2011.02.24.18.59.11	2011.02.24.19.08.12	9 min	Yes
18	F	2	2011.02.28.08.05.41	2011.02.28.08.14.42	9 min	Yes
19	F	2	2011.03.03.11.28.20	2011.03.03.11.38.21	10 min	Yes
20	G	1	2011.03.07.16.11.43	2011.03.07.16.19.44	8 min	Yes
21	H	2	2011.03.11.09.11.22	2011.03.11.09.20.23	9 min	Yes
22	H	2	2011.03.12.17.09.45	2011.03.12.17.19.46	10 min	Yes
23	I	1	2011.03.16.08.55.53	2011.03.16.10.03.54	1 hour 8 min	No
24	J	3	2011.03.18.23.30.41	2011.03.18.23.39.42	9 min	Yes
25	J	1	2011.03.19.09.43.37	2011.03.19.09.52.38	9 min	Yes

The average time to report to US-CERT from the agency headquarters level is 9 minutes, with the exception of two incidents (See Table 2. Duration for Sample Incident Reports, Above). This means 23 out of the 25 incidents have been reported on time. According the Metric ID 003 the percentage of incidents reported on time is 92% (See Figure 10. Percentage of Incidents Reporting on Time, Below). As noted in the comments section for Metric ID 003, management requires 95% compliance for on time incident reporting. With this result, careful consideration is needed to determine the root cause of the problem and possible actions may need to be taken to ensure on time reporting.

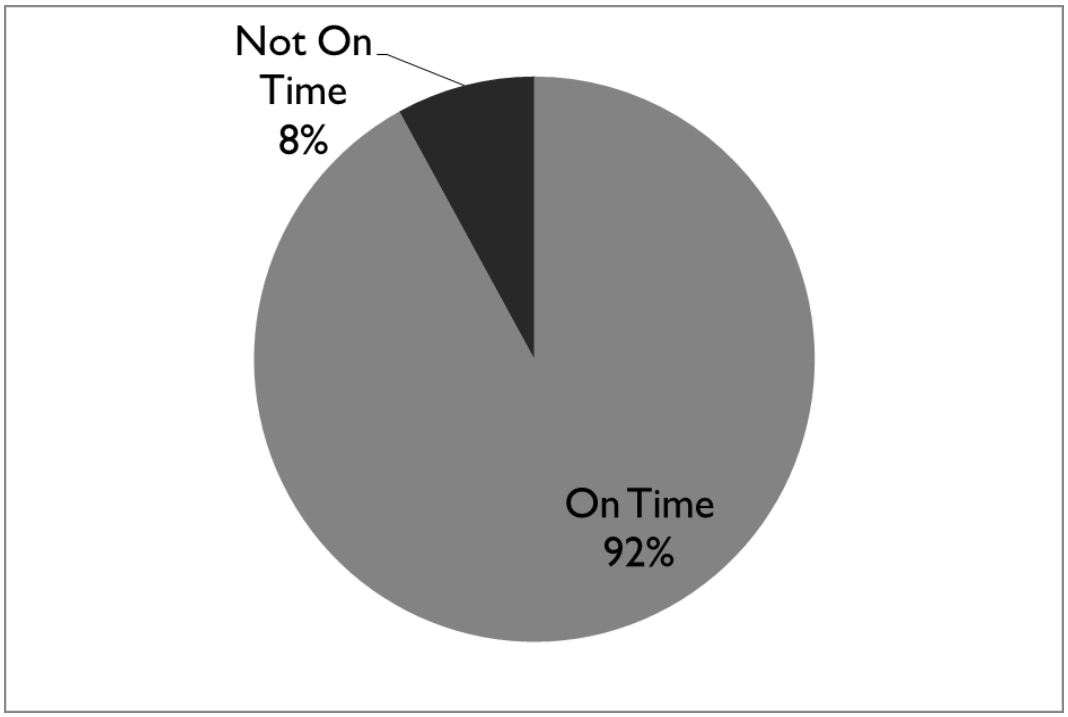


Figure 10. Percentage of Incidents Reporting On Time

ROOT CAUSE

List of Root Causes
Policies not defined
Improper business process design
Improper network architecture
Improper network configuration
Lack of training
Incomplete audits
Insufficient resources
Policies not enforced

Figure 11. List of Root Causes by CERT/CC (Allen, & Davis, 2010)

With further analysis from the case scenario the root cause has been identified. A list of known root causes can be found in Figure 11. List of Root Causes by Computer Emergency Response Team Coordination Center above. By looking at the data set, the bureau where the incident originated from is bureau I. With further investigation the root cause is determined to be the lack of information provided from the incident reported by bureau I. This causes the submission from the agency to US-CERT to be delayed. The policy at the agency level does not clearly outline the minimum requirement to submit via incident category 0-6. Additionally, the policy does not properly utilize category 6 for incidents that are still under investigation.

DECISION BY MANAGEMENT

For this scenario management must decide whether to report incidents to US-CERT even when lacking information or require the bureaus to use category 6 for incidents that are lacking information. The cost measurement is shown in Figure 12. Measurement Form for Metric ID 004 below. Metric ID 004 measures the cost to change policy at the agency level, including the cost to notify and train bureau CSIRTs on using category 6 type incidents.

Incident Response Measurement Form	**Date:** *2011 April, 05 - Tuesday* **Author:** Vincent Sritapan
Metric ID 004	Cost to Change Reporting Procedure
Purpose & Objective	Improve Incident Reporting Process Measure Cost Benefit for Changing Reporting Procedures
Measure Type	*Check all that apply:* ☒ Cost ☐ Time ☐ Quality
Formula	Cost of Policy Change = Rate(Labor Hours for Revision & Notification) + Materials for Notification
Description	Labor rate may vary for revision and notification Materials for notification include training costs to update Bureau CSIRTs
Data Source(s)	Agency CSIRC Bureau CSIRTs (A through J)
Responsible Parties	Agency 1 Headquarters, Division 1 Program Manager: Name ABC Contract Analyst Group: Senior Analyst, Junior Analyst
Audience *Check all that apply:*	☒ Administrative ☒ Operational ☐ External ☐ Other: _____
Frequency	☐ Annual ☐ Monthly ☐ Weekly ☐ Daily ☒ Other: FISMA YEAR
Tie to Agency Mission	Helps organization meet timeframe reporting compliance. Intended for FISMA Audit by DHS.

Comments:

Determine Cost Change Reporting Procedures
Metric ID 001, 002, 003, 004 All grouped for FISMA Audit in Incident Management.

Figure 12. Measurement Form for Metric ID 004

For simplification, the results of Metric ID 004 find that it costs $10,000 to change the policy and notify/train CSIRT staff. Management finds that clearly defining use of category 6 solves the issue of on time reporting.

CONCLUSION

This use case applied five critical elements for developing a metrics framework within CSIR to the timeframe reporting requirements specific to DAs according to US-CERT (See Appendix C). The IR measurement form provided the foundation needed to develop metrics specific to this use case scenario while incorporating the 5 critical elements needed to evaluate CSIR capabilities. The result depicted a

process that measured incident response capabilities and helped identify areas of concern so that risk based decisions could be made to meet management expectations. The use case expressed the importance of the five elements when measuring CSIR and illustrated the how they could be used in a practical scenario. The hope is that this use case will reach middle management in charge of incident response and implementation to measure and improve CSIR could be realized.

REFERENCES

Alberts, C., Dorofee, A., Killcrece, G., Ruefle, R., & Zajicek, M. (2004). Defining incident management process for CSIRTs: A work in progress. *Software Engineering Institute, Carnegie Mellon University*, 7-11.

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

Allen, H. J., & Davis, N. (2010). Measuring Operational Resilience Using the CERT Resilience Management Model. *Software Engineering Institute, Carnegie Mellon University*, 7-15, 23-44.

Center for Internet Security Community (2010). CIS Security Metrics v.1.1.0. *The Center for Internet Security*, 6-39.

Chabrow, E. (2011). Gov't Infosec Incident Soar by 650% in 5 Years. *GovInfoSecurity.com*. Retrieved from http://www.govinfosecurity.com/articles.php?art_id=4114

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*, 12-15, 22-27.

Department of Homeland Security, Office of the Inspector General. (2010). DHS Needs to Improve the Security Posture of Its Cybersecurity Program Systems. *Department of Homeland Security, United States*, OIG-10-111.

Dorofee, A., Killcrece, G., Ruefle, R., & Zajicek, M. (2007). Incident Management Capability Metrics Version 0.1. *Software Engineering Institute, Carnegie Mellon University*, 4-20.

Ellis, J., Fisher, D., Longstaff, T., Pesante, L., & Pethia, R. (1997). Report to the President's Commission on Critical Infrastructure Protection. *Software Engineering Institute, Carnegie Mellon University*, CMU/SEI-97-SR-003, 19-20.

General Accountability Office (2009). Information Security: Agencies Continue to Report Progress, but Need to Mitigate Persistent Weaknesses. *General Accounability Office, United States*, GAO-09-0546.

General Accountability Office (2010). Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative. *General Accounability Office, United States*, GAO-10-338.

General Accountability Office (2011). INFORMATION SECURITY: Weaknesses Continue Abive New Federal Efforts to Implement Requirements. *General Accounability Office, United States*, GAO-12-137.

Hopkins, E. (2009). United State Information and Communication Enhancements Act of 2009. Subcommitte on Federal Financial Management, Government Inforamtion, Federal Services, and International Security.

House of Representatives 245-56. Federal Information Security Management Act of 2002.

NIST (2011). Special Publications (800 Series). Computer Security Division, Computer Security Resource Center, National Institute of Standards and Technology. Link: http://csrc.nist.gov/publications/PubsSPs.html

Payne, C.S. (2006) A Guide to Security Metrics. SANS Institute, 1-3.

Rezmierski, V., Deering, S., Fazio, A., & Ziobro, S. (1998). Incident Cost Analysis and Modeling Project 1: A Report from the CIC Security Working Group to the CIC Chief Information Officers. *Committee on Institutional Cooperation*, 13-15.

Scarfone, K., Grance, T., Masone, K. (2008). Computer Security Incident Handling Guide. *NIST Special Publication 800-61 Revision 1*, 2-16, 3-13, 3-14, 3-26.

Soanes, C., Stevenson, A. (2008). The Concise Oxford English Dictionary, Twelth Edition. "framework n." Oxford University Press, 2008.

Sritapan, V., Stewart, W., Zhu, J., Rohm, T. (2011). Developing a Metrics Framework for the Federal Government in Computer Security Incident Response. Communications of International Information Management Association.

The Internet Engineering Task Force (2011). WG Review: Managed Incident Lightweight Exchange (mile). *The Internet Engineering Task Force*. Retrieved from http://www.ietf.org/mail-archive/web/ietf-announce/current/msg09447.html

US-CERT (2011). Federal Agency Incident Categories. *US-CERT, Department of Homeland Security*. Retrieved from http://us-cert.gov/federal/reportingRequirements.html

Verizon (2010). Verizon Enterprise Risk and Information Sharing Framework. *Security Solutions, Verizon*. Retrieved from https://verisframework.wiki.zoho.com/

West-Brown, J. M., Stikvoort, D., Kossakowski, K., Ruefle, R., & Zajicek, M. (2003). Handbook for Compute Security Incident Response Teams (CSIRTs) 2nd Edition. *Software Engineering Institute, Carnegie Mellon University*, 10-11, 40-55, 191.

White House (2009). Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure. *White House, United States of America*, 1-5.

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.

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, Dorofee, Killcrece, Ruefle, & Zajicek, 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, Deering, Fazio, & Ziobro, 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, Stikvoort, Kossakowski, Killcrece, Ruefle, & Zajicek 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" (General Accountability Office, 2008).

APPENDIX B: ACRONYMS

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

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

US-CERT: United States Computer Emergency Readiness Team

APPENDIX C: US-CERT TIMEFRAME REPORTING

Federal Agency Incident Categories

Category	Name	Description	Reporting Timeframe
CAT 0	Exercise/Network Defense Testing	This category is used during state, federal, national, international exercises and approved activity testing of internal/external network defenses or responses.	Not Applicable; this category is for each agency's internal use during exercises.
CAT 1	*Unauthorized Access	In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource	Within one (1) hour of discovery/detection.
CAT 2	*Denial of Service (DoS)	An attack that *successfully* prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.	Within two (2) hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity.
CAT 3	*Malicious Code	*Successful* installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been *successfully quarantined* by antivirus (AV) software.	Daily Note: Within one (1) hour of discovery/detection if widespread across agency.
CAT 4	*Improper Usage	A person violates acceptable computing use policies.	Weekly
CAT 5	Scans/Probes/Attempted Access	This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.	Monthly Note: If system is classified, report within one (1) hour of discovery.
CAT 6	Investigation	*Unconfirmed* incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.	Not Applicable; this category is for each agency's use to categorize a potential incident that is currently being investigated.

**Defined by NIST Special Publication 800-61*

(US-CERT 2011.)