Appendix B: Example Research-Activity Description

To qualify as a research activity, work must advance the understanding of scientific relations or technologies, address scientific or technological uncertainty, and incorporate a systematic investigation by qualified personnel.

Work that qualifies includes:

- **experimental development** to achieve technological advancement to create new materials, devices, products, or processes, or improve exiting ones;
- **applied research** to advance scientific knowledge with a specific practical application in view;
- **basic research** to advance scientific knowledge without a specific practical application in view; and
- **support work** in engineering, design, operations research, mathematical analysis, computer programming, data collection, testing, or psychological research, but only if the work is commensurate with, and directly supports, the eligible experimental development or applied or basic research.

The following activities **do not** qualify:

- routine data collection;
- development based solely on design or routine engineering practice;
- style changes;
- quality control or routine testing of materials, devices, products, or processes; and
- deployment of a new or improved material, device, or product, or the operational use of new or improved process.

Part 1 – General information

1.1. Fiscal Year: 2013
1.2. Primary point of contact: Mike Smith, Enterprise Security
1.3. Contact person for financial information: Robin Johns, Finance
1.4. Contact person for technical information: Mike Smith, Enterprise Security

The Joint Research Office has defined 19 strategic research contexts, listed below. Brief descriptions of these are provided at the end of this questionnaire. Please select the one below which is the best fit for this requirement.

- ☐ R1 – Mission Management
- ☐ R2 – Computational Platforms
- ☐ R3 – Autonomous and Adaptive Systems
- ☐ R4 – Human–Computer Interaction
- ☐ R5 – Sensor Architecture
- ☐ R6 – Database Systems
- ☐ R7 – Secure System Architecture
- ☐ R8 – Cryptanalysis
- ☐ R9 – Computer Network Analysis
- ☐ R10 – Trusted Computing
- ☐ R11 – Computer Network Defence
- X R12 – Security Measures and Metrics
- ☐ R13 – Secure Communications
- ☐ R14 – Knowledge Discovery
- ☐ R15 – Distributed Computational Space
- ☐ R16 – Advancing Analytics
- ☐ R17 – Systems Engineering
- ☐ R18 – Material Science
- ☐ R19 – Cyber–Physical Systems

Part 2 – Research activity information

Section A - Project identification

2.1. Research activity title (and identification code if applicable): Survey and Experimental Deployment of Security Measures and Metrics
2.2. Activity start date: 2012-09-04
2.3. Activity completion or expected completion date: 2014-04-30
2.4. Field of science or technology code (See CRA SRED program guide for list of codes): (1.02.1) Computer Science
2.5. Is this a continuation of a previously registered activity? No
2.6. Was any of the work (or will any of the work be) done in collaboration with partners? Yes
2.7. If applicable, list names of partners: Carnegie Mellon University
2.8. The work was (or will be) carried out (check any that apply):

- By analysis only; X
- In a laboratory; X
- In a dedicated facility;
- In a commercial plant or facility; and
- Others, specify:

2.9. Purpose of the work:

- To achieve technological advancement for the purpose of creating new or improving existing materials, devices, products or processes. (Go to Section B – Experimental development); or
- For the advancement of scientific knowledge (Go to Section C – Basic or applied research).

This project is focusing on experimental development.

Section B- Experimental Development

2.10. What technological advancements were you (or will you be) trying to achieve? (Maximum 350 words)

Preliminary work has been forthcoming on defining security measures and metrics. The purpose of this project is to collect known measures and metrics into a single compendium (a contribution in its own right) and then to experiment, using our in-house laboratory with combinations of these measurements and metrics so as to determine whether any predictive capacity is produced regarding security posture. Known attacks and vulnerabilities will be simulated and the results of the measurements assessed for their adequacy or to determine why they are failing. There is an expectation that by pursuing this deep analysis, the project will uncover other measurements and metrics worthy of exploration.

2.11. What technological obstacles did you have to (or do you predict will have to be) overcome to achieve those advancements? (Maximum 350 words)

The main obstacle will be the identification of measurements and metrics that are of suitable quality to be worthy of exploration. As has been reported in the literature, many existing approaches are not suitably predictive and, in fact, potentially result in incorrect decisions. Even with suitable exploratory measurements and metrics, determining how to obtain relevant data in a real time basis is expected to be challenging. Finally, it is unclear how we will compose measurements and metrics to enhance predictive power and inform security responses.

2.12. What work did you (or will you) perform to overcome those technological obstacles? (Summarize the systematic investigation) (Maximum 700 words)

At the time of writing this activity report, it was still unclear how these technological obstacles will be overcome. Although we have started collecting industry measurements and metrics and have been reviewing the literature, there are clearly obstacles in instrumenting our laboratory simulation of our enterprise architecture so that the measurements themselves are properly informed. We will be articulating the architecture to the best extent possible and then investigating how to harvest the relevant information in a manner that does not impede normal network behaviour. We will be using state-of-the-art network analysis tools to help in our understandings.

Section C – Basic or applied research

2.13. Describe the scientific knowledge that you were (or you will be) trying to advance. (Maximum 350 words)

N/A

2.14. Summarize the work (or work to be) performed and explain how that work contributed to (or will contribute to) the advancement of scientific knowledge. (Summarize the systematic investigation) (Maximum 700 words)

N/A

Section D – Additional project information

2.15. What evidence do you have (or will you have) to support your work (in case of a review):

- Project planning documents; X
- Records of resources allocated to the project, time sheets; X
- Design of experiments; X
- Project records, laboratory notebooks; X
- Records of trial runs;
- Progress reports, minutes of project meetings;
- Test protocols, test data, analysis of test results, conclusions;
- Photographs and videos;
- Samples, prototypes, scrap or other artefacts;
- Contracts; and/or X
- Others, Specify.

Section E – Intramural Expenditures

2.16. Research and experimental development (R&ED)

In-house	$200,000
Contracts	$50,000
Supporting contracts	$
Grants and contributions	$
Research fellowships	$
Capital expenditures	$

2.17. Related scientific activities (RSA)

Scientific data collection	$10,000
Information services	$10,000
Special services and studies	$
Education support	$5,000
Administration of extramural programs	$1,000
Capital expenditures	$

Section F – Extramural Expenditures

2.18. Research and experimental development (R&ED)

	Business enterprise	Higher education	Canadian non-profit institutions	Provincial and municipal governments	Foreign performers	Other performers
Contracts	$	$50,000	$	$	$	$
Grants and contributions	$	$	$	$	$	$
Research fellowships	$	$	$	$	$	$

2.19. Related scientific activities (RSA)

	Business enterprise	Higher education	Canadian non-profit institutions	Provincial and municipal governments	Foreign performers	Other performers
Scientific data collection	$	$	$	$	$	$
Information services	$	$	$	$	$	$
Special services and studies	$	$	$	$	$	$
Education support	$	$	$	$	$	$

Section G – Personnel

2.20. Personnel engaged in research and experimental development or related scientific activities.

	Engaged in R&ED	Engaged in RSA	Engaged in administration of extramural R&ED programs	Engaged in administration of extramural RSA programs
Scientific and professional (include executive)	2.5 FTEs	FTEs	FTEs	FTEs
Technical	.5 FTEs	.5	.01 FTEs	FTEs
Other	FTEs	FTEs	.01 FTEs	FTEs

Section H – Sources of Funds

2.21. Sources of funds.

Departmental S&T budget (operating and capital and grants and contributions)	$276,000
Total transferred into this program from other departments	$
Total transferred from this program to other departments	$
Net other Federal departments and agencies	$
Provincial government departments	$
Business enterprises	$
Other (please specify)	$