Appendix A. Example Research-Requirement Statement

Note: This is a *simplified* example of a research-requirement statement. A complete statement would hopefully be more concrete, especially regarding success and completion criteria.

Section 1: Identification/Criticality

Please provide the date of completing this questionnaire, a title for the research requirement, the point(s) of contact for this questionnaire, and your perception of the urgency and importance level of the requirement.

Date (YYYY-MM-DD)	2012-06-24
RRS #	ORG-SEC-024
Requirement Title	Security Measures and Metrics
Point of Contact & Group	Mike Smith, Enterprise Security
Urgency Timeline	**X** Short term ☐ Medium term ☐ Long term
Importance	☐ Low ☐ Medium **X** High

Section 2: Stakeholders

We identify three kinds of stakeholders:

1. *An operational stakeholder (who may actually deploy the results);*
2. *A technical stakeholder (who provides technical development or advancement); and*
3. *A subject matter expert.*

Normally, the first two stakeholders are business groupings and the SME an individual. More than one entity or person can be identified within the stakeholder options.

Operational Stakeholder(s)	Information Operations
Technical Stakeholder(s)	Enterprise Security
Subject-Matter Expert(s)	Mike Smith and John Doe

Section 3: Business Description

What are the business motivations (strategic goals, specific objectives) that are to be addressed by this requirement? Please consider describing the existing or potential general business context of the requirement, identifying existing or proposed business functions that will be impacted and how they will be impacted.

1. The corporate costs associated with information-technology security have been rising and are drawing the attention of executives. It has been increasingly difficult to choose among options as the benefits/costs/tradeoffs are poorly understood.
2. Recent unfortunate experiences suggest that the corporation's infrastructure is not agile in responding to attacks. There is a need for enhanced, well-informed situational awareness of our security status and the ability to respond automatically to attacks.
3. Attempted theft (apparently successful on occasion) of our trade secrets has the potential to seriously impact our revenues and business advantage. The current status quo is no longer tenable.

Section 4: Research Requirement

Please provide a short description of the research requirement and how it relates to the business motivations. Identify the most significant technical challenges that must be resolved to achieve the objectives of the research requirement. Provide a synopsis of the core technical issues, and a synopsis of proposed solutions or approaches. What other research requirements or activities are related to this requirement?

Advancing the state of scientifically sound security measures and metrics would greatly aid the design, implementation, and operation of secure information systems. Specifically, by improving our knowledge of our enterprise security architecture we will be in a better position to respond to organizational needs. Our overall requirement is to have automated gathering of network data to rapidly assess the overall security posture of the enterprise. A critical enabler will be to meaningfully quantify this assessment with relevant metrics.

Section 5: Success / Completion Criteria

How will you know that the research requirement has been resolved? Please describe what would be considered a success.

Given the nascent nature of research into scientifically grounded security measures and metrics, it is somewhat difficult to fully capture success and completion criteria. Having said that, success will be achieved if we have measurements that are continuously monitoring the security posture of the system; that these measurements meaningfully (are scientifically based) reflect the security posture; and that both manual and automated responses to appropriate classes of threats are suitably informed. Furthermore, the ability to model our enterprise and perform well-founded reasoning on security and business investments will be a major step forward.

Section 6: Category Impact

This research will primarily impact (please select only one):

- **X** Enterprise Operational Capabilities
- ☐ Partner Operational Capabilities
- ☐ Enterprise Research Capabilities

Its impact on the capabilities will be (please select only one):

- ☐ Low
- ☐ Medium
- **X** High

Section 7: Description of Impact

Please describe why and how you expect the Research & Experimental Development (R&ED) to enable the operational or research capabilities of the enterprise or its partners.

It is expected that a focused research effort on security measures and metrics will lead to enhanced understanding of our IT infrastructure, will identify attack vectors, vulnerabilities, and better inform what system data is required to properly inform evolving measurements. The impact could be substantial because, through scientifically-based measurements, the organization will be better informed in making security investment decisions and their relationship to other organizational imperatives. Furthermore, through a sound understanding of the posture of our enterprise architecture, we can more confidently respond to attacks or evolving vulnerabilities and threats. The increased cost-effectiveness and agility of our responses will materially impact our bottom line while enhancing our security posture.

Section 8: Relationship to Strategic Research Contexts

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
- ☐ R19 – Cyber–Physical Systems
- ☐ 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

Section 9: Partnerships

To your knowledge, please specify and describe any inside or outside organizations (Canadian Government, partners, industry, academia, etc.) that are either working or have manifested an interest in a similar research requirement.

Extensive research in security measures and metrics are underway in a number of U.S. universities. NCSU, Carnegie Mellon, and University of Illinois at Urbana–Champaign are focusing on grand challenges related to the science of security that include security measures and metrics. Lincoln Laboratories recently published a report on continuous security metrics. There is a need to investigate current industry practice and relate practice to research trends.

Section 10: Notes

Any clarifications, questions, etc., you wish to include.