Refresh Knowledge, Renew Commitment, and Refocus Efforts
Crowdsourcing to Discover Lost in Translation Requirements

Breakout Session #E02
Mike Ipsaro, Technical Director, Integrity Management Consulting

December 13, 2016
Tuesday, 2:15PM–3:30PM
Agenda

1. Purpose
2. What could go wrong and why?
3. The art and science of requirements
4. Crowdsourcing in action
5. Can tailored crowdsourcing work for us?
PURPOSE

To dialogue about the art and science of requirements, particularly definition, including the application of the crowdsourcing concept to it.
Successful acquisition outcomes

• Enables Mission accomplishment
• Customer satisfaction, stakeholder acceptance
• Legal, regulatory, and policy compliance
• Demonstration of stewardship

Enabled by completeness and accuracy of requirements
Agenda

1. Purpose
2. What could go wrong and why?
3. The art and science of requirements
4. Crowdsourcing in action
5. Can tailored crowdsourcing work for us?
WHAT COULD GO WRONG AND WHY?

From the program/project perspective
What could go wrong

And from the perspective of the contract
Technically and non-technically speaking

Why do you think requirements get lost in translation or are just never found in the first place?
Inherent, common challenges

1. Longstanding communication paradigm
2. Many stakeholders
3. Many requirements
Generic acquisition process

Plan & Define (Requirement) → Solicit → Source Selection → Administration

Longstanding communication paradigm
Many Stakeholders

• Many perspectives and perceptions
Many requirements (documents)

Generally speaking, Requirement documents can be viewed on spectrum, from general to specific, qualitative to quantitative, or from operational to technical.

• Strategic Goals
• Mission Need Statement (MNS)
• Operational Requirements Document (ORD)
• Functional and System Requirements Document (FRD)
• Specifications (Design, Material)
• Statement of Work/Objectives / Performance Work Statement (PWS)
Many Requirements within document(s) (e.g., generic SOW)

1. Requirement Information
2. Section II – Purpose
   • Product, Service, or Outcome Required
   • Scope of the Product, Service, or Outcome
3. Background
4. Technical Requirements/Tasks/Outcomes
   • Deliverables
   • Special Delivery Instructions
   • Performance/Delivery Period
   • Place/Location of Performance/Delivery
   • Travel Requirements
   • Special Requirements
5. Section V – Applicable Documents
6. Section VI – Requirements for Handling Sensitive, Classified, and/or Proprietary Information
7. Section VII – Government-Furnished Resources and Information
8. Section IX – Performance Requirements/Quality Assurance Surveillance Plan (QASP)
   • Acceptable Quality Levels (AQLs)
   • Evaluation/Surveillance Methods
   • Incentives/Awards
9. Section X – General Contact Information

How do you approach this complexity?
Agenda

1. Purpose
2. What could go wrong and why?
3. The art and science of requirements
4. Crowdsourcing in action
5. Can tailored crowdsourcing work for us?
ART & SCIENCE

Approaching complexity of Requirements requires a blended approach
Asking the right questions (Define)

• What functions must the product/service perform?
• How well do the functions have to be performed?
• What characteristics, assumptions, constraints surround the functions?
• In what environment must the product perform?
• With what must the product interface?
• What are the sustainment issues?
• Is the requirement SMART?

Definition = Effective Communication
Asking the right questions at the right time

Redesigned/recast to change communication paradigm
Asking the right questions in the right way

- Understand and capture the perspectives behind the requirements
- How can you do that?

Effective Communication = Mutual Understanding
PERCEPTION

Could be the most important factor in understanding

- Textual vs. Contextual?
- Perhaps, single biggest reason of communication problems is misperception.
- Two people look at same picture, but each sees a different part.
- Two people look at same part but sees it differently.
- Different strokes for different folks

Understanding = seeing the picture(s) in the other’s head
Perception and Reality

Are they always the same?
I think therefore I am
What’s the difference?

“We Don’t See Things As They Are,

We See Them As We Are.” - AN

0 if we both see it’s 1?
Are we both right?

How about we agree to disagree?
Orchestration

Many *different* people playing *different* instruments.....

......but from the *same* sheet of music
Agenda

1. Purpose
2. What could go wrong and why?
3. The art and science of requirements
4. Crowdsourcing in action
5. Can tailored crowdsourcing work for us?
What is Crowdsourcing concept?

Here is what Meriam says...

“the practice of obtaining needed services, ideas, or content by soliciting contributions from a large group of people and especially from the online community rather than from traditional employees or suppliers”.
The concept is all around us

• Wiki, Yelp, Waze, DHS “see something, say something”, Intellipedia

Can the crowdsourcing concept be *tailored* or adapted?

Agenda

1. Purpose
2. What could go wrong and why?
3. The art and science of requirements
4. Crowdsourcing in action
5. Can tailored crowdsourcing work for us?
Taileored Crowdsourcing in action across the spectrum...

• Crowdsourcing principles at all levels to enable better requirements definition
  • NIST Cybersecurity Framework
  • DHS Strategic Principles
  • President’s Cybersecurity Commission
  • OMB Mythbuster’s campaign
  • Organizational level requirements management
  • Working group/tactical micro level (building a requirements document)
Rosetta Stone
## Critical Infrastructure Sectors

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Chemical</td>
</tr>
<tr>
<td>2.</td>
<td>Commercial Facilities</td>
</tr>
<tr>
<td>3.</td>
<td>Communications</td>
</tr>
<tr>
<td>4.</td>
<td>Critical Manufacturing</td>
</tr>
<tr>
<td>5.</td>
<td>Dams</td>
</tr>
<tr>
<td>6.</td>
<td>Defense Industrial Base</td>
</tr>
<tr>
<td>7.</td>
<td>Emergency Services</td>
</tr>
<tr>
<td>8.</td>
<td>Energy</td>
</tr>
<tr>
<td>9.</td>
<td>Financial Services</td>
</tr>
<tr>
<td>10.</td>
<td>Food and Agriculture</td>
</tr>
<tr>
<td>11.</td>
<td>Government Facilities</td>
</tr>
<tr>
<td>12.</td>
<td>Healthcare and Public Health</td>
</tr>
<tr>
<td>13.</td>
<td>Information Technology</td>
</tr>
<tr>
<td>14.</td>
<td>Nuclear Reactors, Materials, and Waste</td>
</tr>
<tr>
<td>15.</td>
<td>Transportation Systems</td>
</tr>
<tr>
<td>16.</td>
<td>Water and Wastewater Systems</td>
</tr>
</tbody>
</table>

How do you communicate or translate Cybersecurity Requirements in 16 languages?
A framework for requirements

How do you define cybersecurity requirements?
A kind of rosetta stone

The Framework is risk-based, and is composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers.

<table>
<thead>
<tr>
<th>Function Identifier</th>
<th>Category Identifier</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>ID.AM</td>
<td>Asset Management</td>
</tr>
<tr>
<td></td>
<td>ID.BE</td>
<td>Business Environment</td>
</tr>
<tr>
<td></td>
<td>ID.GV</td>
<td>Governance</td>
</tr>
<tr>
<td></td>
<td>ID.RA</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td></td>
<td>ID.RM</td>
<td>Risk Management Strategy</td>
</tr>
<tr>
<td></td>
<td>PR.AC</td>
<td>Access Control</td>
</tr>
<tr>
<td></td>
<td>PR.AT</td>
<td>Awareness and Training</td>
</tr>
<tr>
<td></td>
<td>PR.DS</td>
<td>Data Security</td>
</tr>
<tr>
<td></td>
<td>PR.IP</td>
<td>Information Protection Processes and Procedures</td>
</tr>
<tr>
<td></td>
<td>PR.MA</td>
<td>Maintenance</td>
</tr>
<tr>
<td></td>
<td>PR.FT</td>
<td>Protective Technology</td>
</tr>
<tr>
<td></td>
<td>DE.AE</td>
<td>Anomalies and Events</td>
</tr>
<tr>
<td></td>
<td>DE.CM</td>
<td>Security Continuous Monitoring</td>
</tr>
<tr>
<td></td>
<td>DE.DP</td>
<td>Detection Processes</td>
</tr>
<tr>
<td></td>
<td>RS.RP</td>
<td>Response Planning</td>
</tr>
<tr>
<td></td>
<td>RS.CO</td>
<td>Communications</td>
</tr>
<tr>
<td></td>
<td>RS.AN</td>
<td>Analysis</td>
</tr>
<tr>
<td></td>
<td>RS.MI</td>
<td>Mitigation</td>
</tr>
<tr>
<td></td>
<td>RS.IM</td>
<td>Improvements</td>
</tr>
<tr>
<td></td>
<td>RC.RP</td>
<td>Recovery Planning</td>
</tr>
<tr>
<td></td>
<td>RC.IM</td>
<td>Improvements</td>
</tr>
<tr>
<td></td>
<td>RC.CO</td>
<td>Communications</td>
</tr>
</tbody>
</table>

- **TIER 1** Partial
- **TIER 2** Risk Informed
- **TIER 3** Repeatable
- **TIER 4** Adaptive

**Informative References**
- CCS 5101
- COBIT 5:2012
- ISA 5.40:2009
- ISO/IEC 27001:2013
- NIST SP 800-53 Rev. 4

**Identify (ID)**
- Asset Management (IDAM): The data, processes, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization’s risk strategy.
Requirements for the Framework

Enabled through tailored crowdsourcing
Other recent examples

COMMISSION ON ENHANCING NATIONAL CYBERSECURITY
DECEMBER 1, 2016
REPORT ON SECURING AND GROWING THE DIGITAL ECONOMY

U.S. Department of Homeland Security

STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS (IoT)

Version 1.0
November 15, 2016
CROWDSOURCING IN ACTION

In addition to the adaptation of crowdsourcing at the macro level, it can be adapted at more micro levels.

1. **Organizational level:**
   - People/teams, practices, tools (sharepoint), training
   - Communication paradigm (Draft) RFIs, Draft RFPs, Vendor Conferences (online) as part of market research
   - IPTs including users, A/B testing, data analytics

2. **Requirements Document/Writer level:**
   - Writing Contract-level requirements docs (SOWs, SOOs)
Organizational Level

People
Process
Tools
Writer level - guidelines

✓ Think – What, when, where, how (how many, how much, how well...)
✓ Think outcomes ("what you want") vs. Process ("how to do it")
✓ Think alignment
MEMORANDUM FOR CHIEF ACQUISITION OFFICERS
SENIOR PROCUREMENT EXECUTIVES
CHIEF INFORMATION OFFICERS

FROM: Lesley A. Field
Acting Administrator for Federal Procurement Policy

SUBJECT: “Myth-Busting 2”: Addressing Misconceptions and Further Improving Communication During the Acquisition Process

Early, frequent, and constructive engagement with industry leads to better acquisition outcomes, which is why it is one of the key tenets of the Office of Management and Budget’s 25 Point Implementation Plan to Reform Federal IT Management. Such engagement is especially important for complex, high-risk procurements, including (but not limited to) those for large information technology (IT) projects.

To that end, the Office of Federal Procurement Policy (OFPP) last year issued the “Myth-Busting” memorandum on “Addressing Misconceptions to Improve Communication with Industry during the Acquisition Process.” In the subsequent months, Federal agencies have taken significant additional steps to improve communications between Federal agencies and the vendor community. These developments are discussed further below.

To continue to make progress in improving these communications, OFPP is issuing this second “Myth-Busting” memorandum. Whereas we focused last year on the misconceptions on the part of Federal agencies, we want to continue the discussion by addressing in this memorandum the misconceptions that may be held by some in the vendor community. As we did last year, we highlight the misconceptions in the Attachment and, for each one, provide the facts about the Federal procurement process, with the goal of improving the productivity of our communications. The Attachment also provides additional information and strategies for both agencies and vendors to promote more effective communication.

We encourage you to share this information with current and potential industry partners—especially those new to government contracting—as part of your outreach efforts to ensure that we are collectively making the best use of our engagement opportunities.
• Current Proposed Federal Rule
• Federal Register Vol. 81, No. 229 / 29 NOV 2016. FAR Case 2016-005
• FAR: Effective Communication between Government and Industry
Contact Information

Mike Ipsaro
703.216.0538 (mobile)
mipsaro@integritymc.com
References

• DAU Requirements/SOW class
• NIST Cybersecurity Framework
• Presentation on developing NIST framework
• DHS Strategic Principles of Cybersecurity
• Google images
• Wikipedia
• Wharton School of Business Negotiation class - *Getting More* by Stuart Diamond
• OMB Mythbusters Memo
• Federal Register Volume 81