AEROSPACE REPORT NO.
TOR-2014-02201

Technical Risk Identification at Program Inception

April 20, 2014

Andrew Y. Hsu[1] and Amy Weir[2]
[1]Acquisition Risk and Reliability Engineering Department, Mission Assurance Subdivision;
[2]Program Executability, Engineering Directorate

Prepared for:

National Reconnaissance Office
14675 Lee Road
Chantilly, VA 20151-1715

Contract No. FA8802-14-C-0001

Authorized by: National Systems Group

Developed in conjunction with Government and Industry contributions as part of the U.S. Space Program Mission Assurance Improvement Workshop.

Acknowledgments

This document was produced as a collaborative effort of the Mission Assurance Improvement Workshop. The forum was organized to enhance Mission Assurance processes and supporting disciplines through collaboration between industry and government across the US space community. The MAIW engages the appropriate subject matter experts to share best practices across the community in order to produce valuable mission assurance guidance documentation.

The document was created by multiple authors throughout the government and the aerospace industry. We thank the following contributing authors for making this collaborative effort possible:

Robert Ellsworth	The Boeing Company
Robert Jennings	Raytheon Company
Debra Olejniczak	Northrop Grumman Corporation
Larry Rubin	SSL
Jerome Sobetski	Lockheed Martin Space Systems

A special thank you for co-leading this team and efforts to ensure completeness and quality of this document goes to:

William Frazier (Co-Lead)	Ball Aerospace
Andrew Hsu (Co-Lead)	The Aerospace Corporation
John McBride (Co-Lead)	Orbital Sciences Corporation
Amy Weir (Co-Lead)	The Aerospace Corporation

The Topic Team would like to acknowledge the support, contributions and feedback from the following organizations:

Ball Aerospace
The Boeing Company
Booz Allen Hamilton Inc.
Lockheed Martin Space Systems
Northrop Grumman Corporation
Orbital Sciences Corporation
Raytheon Company
SSL

The authors deeply appreciate the inputs of the subject matter experts who reviewed the document and made valuable contributions to the final product:

Alexis Burkevics	Aerojet Rocketdyne
Anh Dang	The Aerospace Corporation
Jaclyn Decker	Orbital Sciences Corporation
Sergio Guarro	The Aerospace Corporation
Ben Hoang	Orbital Sciences Corporation
David Pinkley	Ball Aerospace
Dennis Rubien	Northrop Grumman Corporation
LaKeisha Souter	Northrop Grumman Corporation
Brian Weir	Booz Allen Hamilton Inc.

Executive Summary

> *"....as we know, there are known knowns; there are things that we know that we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns, the ones we don't know we don't know."*
>
> —Donald Rumsfeld, United States Secretary of Defense

Since many risks realized are not identified, this paper examines the barriers to comprehensive risk identification, recommends methods for overcoming these barriers, and provides other best-practices for improved risk identification. These recommendations target the unidentified technical risks to program and mission success that can and should be identified at program inception (concept definition and proposal development through the preliminary design). The recommendations may also improve risk identification throughout the program lifecycle.

Contents

Figures

Tables

1. Purpose

> *"Total Risk is the sum of identified and unidentified risk. Some unidentified risks are subsequently identified when a mishap occurs. Some risk is never known."*
>
> - FAA Risk Management Handbook, FAA-H-8083-2

Risk *management* is a robust and well documented process applied in commercial industries and government programs and risk *identification* is an important first step in the process. Problems were frequently not previously identified as risks and therefore the methods and tools available to manage those risks were not implemented. The purpose of this document is to help the space community recognize barriers that inhibit effective baseline risk identification, and provide methods to help customers and contractors more effectively address these barriers. Specifically this document is targeted at prime and subcontracting agents, risk process owners, and risk management practitioners.

Total risk identification for any program is neither practical, nor is it absolutely measurable. Approaches to provide an indication of the completeness of risk identification are described in this document. Utilizing the recommended methods can provide a good indication of the unidentified risk exposure at program inception and throughout the lifecycle (see Figure 1).

Once identified, each risk can be assessed, and the program can either consciously accept it or plan to mitigate, track, and report status using established tools and methods. The Risk Management activities after identification are unique to each organization, customer, product line, or program, and are not within the scope of this document.

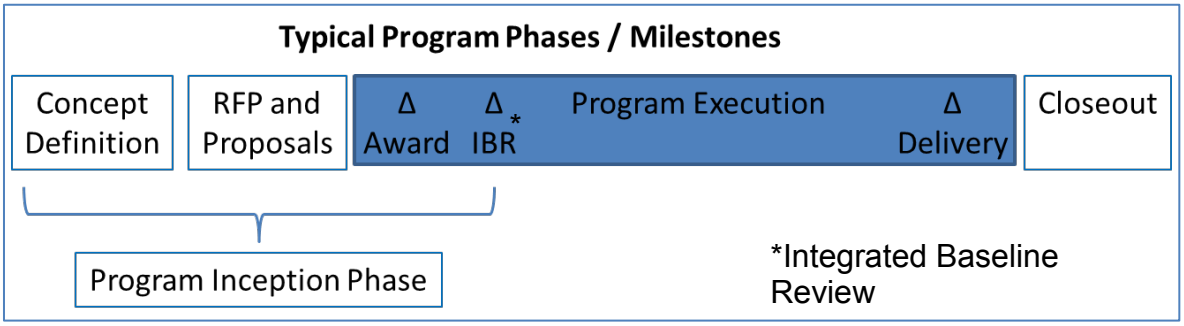


Figure 1. Typical program phases.

2. Current State of Risk Identification in the Space Industry

> *"The major difference between a thing that might go wrong and a thing that cannot possibly go wrong is that when a thing that cannot possibly go wrong goes wrong it usually turns out to be impossible to get at or repair."*
>
> - The Hitchhiker's Guide to the Galaxy, Douglas Adams

Over time modern space systems' technical practices have evolved to improve the predictability of achieving the target outcomes. The disciplines of engineering, quality, reliability, contamination control, parts, materials, and processes, safety, and others have improved their design standards and processes to mitigate commonly realized risks. The improvement in these disciplines does not make continual risk identification obsolete – especially for development and new technology programs.

There are many barriers to effective risk identification. By working to overcome these barriers, a program can improve the identification of risks and efficiently implement risk mitigation strategies.

The space industry already has risk identification methods (see Table 1). These are grouped into methods based on personal experience and knowledge (experiential) and methods based on analysis of data (analytical). Each method has advantages and disadvantages. Effective risk identification usually requires a combination of two or more methods to overcome the disadvantages.

Table 1. Risk Identification Methods

Risk ID Method	Description	Strengths	Weaknesses
Experiential Methods			
Review previous program risks, issues, and lessons learned	Review of risks and issues identified on prior programs of similar scope, complexity, and use of technologies to see if any are applicable to the current program	Leverages relevant knowledge from similar programs.	May not include risks outside of prior programs' experiences. Differences between programs may not be understood.
Checklists and questionnaires	Structured method to identify known potential risk areas based on past experience, and to have responders assess the applicability of those potential risks to the current program.	Leverages institutional and organizational lessons learned.	May not identify risks outside of the group's prior experiences. Requires organization repository and maintenance.
Brainstorming	Utilizes social interaction to enhance the risk identification process. It requires a competent and unbiased facilitator to help keep the discussion on topic.	Provides a structured method to leverage the knowledge breadth of a diverse group of experts.	Dominating individuals may attempt to push their ideas onto the rest of the group, and weaker personalities might not get a chance to air their views. Only as good as the experience breadth of the group.
Personal knowledge/ experience of risks	Collect risks based on one or more individual's personal knowledge and expertise. Example questions "What are you worried about? What keeps you up at night?"	Beneficial within each individual's experience range.	Limited team experience or knowledge. Individuals can inject biases into process. May not capture institutional experience lost with attrition. May not translate experience, design weakness, etc. into a risk framework.

Risk ID Method	Description	Strengths	Weaknesses
Analytical Methods			
Key Performance Parameters (KPPs) – technical, programmatic	Review of the KPPs to identify the specific risks to achieving the key program objectives. Monitor trends in KPPs and margins/reserves.	Provides risk identification that is targeted on the design's ability to meet the program's KPPs.	Assumes the program's identified KPPs fully represent the parameters that best represent the required system performance.
Review Project Work Breakdown Structure (WBS)	A critical review of the WBS can expose risks inherent in the interdependency of the project work.	Provides a structured approach for risk identification in the context of how the program's work is structured, including entities external to the program (suppliers, teammates, governmental entities, etc.).	Risk identification using the WBS is only as good as the WBS itself, and the expertise of the risk identifiers reviewing the WBS.
Risk Breakdown Structure	Risks are stated and assessed at each level of architectural assembly: system, subsystem, unit, component and part. Higher level risk assessments are informed largely by historical data. Middle level risks also include the risk of interface and interaction. Component and part level risks are only assessed for very high unit-level risks.	Comprehensive, structured, and intuitive for the reviewer. Aggregate risks include the probabilistic sum of all of the constituent elements.	Aggregation is subjective, and typically not statistical or mathematical – resulting in decreased confidence. Low aggregate risks may mask high concentrations of risk in certain components or parts. Effective mitigation is sometimes best performed at a different level than the level being reviewed.
Inception Risk Standardization	Each program assesses and dispositions a list of pre-defined standard risks based on the experience and data collected from historical programs and missions.	This method requires programs to assess likely risks which may be overlooked.	Pre-defined standardized risk lists are not likely to be insightful to mission and program specific risks.
Review Requirements, Design Documents, and Drawings	Review of these documents can reveal perceived gaps in the design, or over-constraints that could adversely affect design development.	Provides a structured approach for risk identification in the context of the program's requirements and design documentation.	Risk identification using the requirements and design documentation is only as good as the documentation itself, and the expertise of the risk identifiers reviewing the documentation.
Utilization of Models and Simulations	Early models and simulations can help identify weak points in the requirements or the design, and help direct programmatic attention to address concerns before they manifest as design issues.	Models and simulations provide early insight into the design and its performance, from which risks (and issues) can be identified and documented.	Risk identification using models and simulations depends on how well they correlate to the actual design, level of realism, and the expertise of the risk identifiers analyzing and interpreting the results.
Fault Tree Analysis (FTA) and/or Root Cause Analysis (RCA)	FTA provides insight into design weaknesses and helps the engineering team identify added mitigations that may prevent faults or minimize impact of faults. RCA provides insight into process weaknesses and helps organizations add mitigations that may prevent fault recurrence.	FTA and RCA provide a rigorous methodology to understand potential contributors to a given fault. The process could help inform the analyst as to where a design is exposed to otherwise unidentified risks.	Risk identification during the FTA or RCA process depends on the depth and breadth of the analysis, and the expertise of the analyst. RCA responds to the presence of a failure and can be useful in predicting recurrence, but are not useful in predicting first occurrence.

Risk ID Method	Description	Strengths	Weaknesses
Analytical Methods			
Failure Modes and Effects Analysis (FMEA)	FMEAs help identify where design is exposed to failure modes, and inform the program on technical risks, consequences, and need for added mitigation.	FMEA provides a rigorous methodology to identify and understand the failure modes of a given design. This better informs the program's risk identification process both at the unit/subassembly level, as well as at the system level.	Risk identification during the FMEA process depends on both the rigor applied to the FMEA, and the systemic understanding of how a unit's failure modes/effects will impact performance of the larger system.
Review of Test Plans or Test Results	Test plan reviews (for breadth and depth of testing) help to identify where a system test plan may be inadequate in ensuring requirements are addressed and properly verified. Test results reviews help to identify if risk has been realized, and may also inform the engineer of unexpected performance attributes that pose potential risk to system performance.	Reviewing test plans in the context of risk identification can provide the reviewer insight into verification risks. Reviewing test data in the context of risk identification can provide the reviewer the first opportunity to assess any unexpected actual performance of the element under test, and evaluate its potential risk to the larger system.	Risk identification derived from Test Plan reviews tend to focus only on what is tested (as opposed to what is not tested). For test data reviews, a reviewer may unintentionally mask a discovered issue as a risk.
Assessing exceptions to mission assurance standards and processes	An evaluation of tailorings, waivers, or deviations from customer or enterprise required mission assurance standards and processes to assess risk potentially introduced by these exceptions.	Establishes risks relative to an accepted baseline. Performing to modified standards may have inherent risks, unidentified.	None

3. Barriers to Risk Identification

There are many barriers to risk identification commonly encountered within the space community. Some of these barriers are intrinsic to an organization's processes, some are the result of contractual relationships between customer and contractor, and others are inherent in human psychology. These barriers impact the ability of customers, contractors, and risk practitioners to effectively identify risks. Recommended actions to mitigate the risk barriers described below are provided in Section 5.

3.1 Barrier 1: Over-Reliance on a Single Method

> *Experts in the psychology of human error have long been aware that even highly trained experts are easily misled when they rely on personal experience and informal decision rules to infer the causes of complex events.*
>
> -Barry Beyerstein, Professor of Psychology

Most programs typically rely on personal experience as the primary or even the sole risk identification method. This experience is a rich source of knowledge of potential adverse consequences. However history also shows that many risks realized were not part of the experience set of those personnel, and were therefore neither identified nor mitigated. Other risk identification techniques such as brainstorming can improve collective recall, but they still rely primarily on the collective experience of the team members polled. Consequently, human psychology results in the incorporation of Normalcy Bias (i.e., "it's been OK before"), bounded rationality (limited information/cognitive abilities), and epistemic failures (bad decisions).

The program should use a diversity of experiential and analytical techniques and should assess risk identification completeness, and management/customer should periodically review this measure.

3.2 Barrier 2: Artificial Constraints and Biases

> *Many program managers, especially those facing more problems than they can handle, unconsciously signal to their teams that they do not want to hear about any new risks, even if they explicitly support good risk management processes. Their teams thus become reluctant to identify and report risks even though they could significantly affect the project.*
>
> Overcoming Cultural Obstacles to Managing Risk, by Daniel Galorath

Management frequently establishes artificial constraints that act as barriers to the program team's ability to effectively identify risks at program inception. Examples of such constraints are:

- Limiting the total number of risks identified. Program investment in risk identification is not unlimited, and an inevitable constraint occurs when the volume of risks identified strain the ability to manage them.
- Bias towards identifying a large aggregated risk can mask its constituents. Aggregated risks which combine multiple causes or effects attract significant program attention, and smaller risks that may be more effectively mitigated may go unidentified.

- Bias towards identifying many small individual risks or failure to look across those individual risks may mask their relationships and interdependencies.
- Self-censoring risks with no apparent available mitigation. Risk identifiers are frequently reluctant to identify, track, and report risks that they assume to be implicitly accepted (e.g., use of heritage designs, risk of damage during launch environment).
- Establishing a quota of high, medium, and low risks (e.g., "As a low risk program there should only be low risks identified.").
- Establishing program areas where risk identification is not welcome (e.g., recurring designs, customer specified interfaces, or areas of corporate reputation).
- Misidentifying issues as risks may limit the robustness of risk identification.

Risk practitioners should assess the constraints and biases facing the program and implement mitigations against them.

3.3 Barrier 3: Dismissing a Risk as a Normal Program Challenge

> *"You want to know what my IPT's risk is in executing our design development plan? I have a great team, and I know we can figure out how to make this work, I don't see any risk."*
>
> -Anonymous IPT Lead

In all development programs there are challenges. Design development and verification are part of the program, and there are usually varying degrees of confidence in meeting the technical challenges. The yet undiscovered hurdles may be viewed as normal program activity, or they may be seen as technical risk. Differentiating technical risk from routine technical activity at program inception is a matter of perception.

The overconfident program manager may fail to recognize the technical risks in their normal development, and may therefore be insufficiently prepared to mitigate them. The program that over-identifies uncertainty as risk is likely to overwhelm the risk management process.

The balanced program approach carefully reviews the program's planned activities, anticipates the unintended results, and discriminates the risks from planned activities. The most significant risks are those that can persist beyond their retirement deadline. Programs should carefully review their technical challenges in light of the program commitments and constraints (cost, schedule, resource, etc.) and extract the technical risks that may be inherited by the next phase – especially delivery to orbit.

3.4 Barrier 4: Compliance Reliance

> *"We implemented our approved, standard processes. I did not expect this problem."*
>
> -Anonymous Mission Assurance Executive

Space industry and proprietary standards, processes, and procedures have been developed to ensure that program deliverable products and services will meet an array of requirements – that they are fit

for their purpose, are safe, reliable, and of good quality, and have characteristics or meet certain requirements for performance, commonality, interoperability and compatibility with other systems, and similar objectives. Standards provide requirements, specifications, guidelines, or characteristics that result from technical considerations, and include, but are not limited to, definitions and terminology, methods and criteria for measurement and test; ratings structures; application guides; recommended practices; design margins; and specific materials, processes, and procedure requirements.

Adhering to the definitive set of engineering practices for the program would seem to ensure that the products developed will perform as required. Social scientists describe this phenomenon as "compliance reliance".

However, space programs are inherently complex, and merely adhering to a set of engineering documents does *not* ensure that the system as a whole will meet requirements. Complex engineering projects may differ greatly from the "sum of the parts" properties – with behaviors and interactions among system components that are quite different than expected. Additionally, despite rigorous methods, part procurement problems, process inconsistencies, workmanship errors, and other issues at lower levels still occur. The failure to appreciate the sensitivity of system level to lower level performance is a barrier.

Therefore, regular risk ID check-ups should include use of standardized checklists, and assessment of overall systems engineering rigor.

3.5 Barrier 5: Program Acquisition Attributes

> *"The government will evaluate proposals deemed acceptable to ascertain both the degree of Technical Risk and the reasonableness of the proposed price."*
> -U.S. Government Request for Proposal

The acquisition process can create barriers to the identification of risk. The language within the Request for Proposal (RFP) can significantly shape the bidder's proposal. If the RFP requires that certain key risk areas be addressed, the proposal will focus on those risks, potentially to the exclusion of others. Likewise, since the source selection process often rewards a low risk offering, a proposal will tend to project low risk. This low risk posture becomes the baseline for the program, inhibiting expansion of or reassessment of the risk landscape.

The contractor and customer should instead establish a cooperative and collective interest in understanding the complete risk profile. Risk identification workshops (using selected methods from Table 1) conducted within each organization, and as integrated teams, should provide thorough, meaningful risk identification.

3.6 Barrier 6: Scope Boundaries

> *"Risk is a Borderless Phenomenon."*
> -Denis Smith and Moira Fischbacher, Editors, Risk Management Journal

Some risks are not identified because they are perceived to be outside of identifiers' scope; the potential problems are "not in my backyard". Examples of these scope boundary barriers include

system interfaces within a contractor scope or crossing customer and contractor boundaries (e.g., spacecraft-to-LV, spacecraft-to-ground segment, or payload-to-spacecraft), program funding, potential for obsolescence to affect follow-on production, and product dependencies (e.g., GFE, Operations Center availability).

The risk identification process should consider all system interfaces and assumptions, both internal and external to the system. It should also consider investigating the "fringes" of the system, even if marginally out of scope. Programs should utilize inter-element forums to solicit risks from outside of assigned scopes.

3.7 Barrier 7: Normalization of Deviance

> *"Social normalization of deviance means that people within the organization become so much accustomed to deviant behavior that they don't consider it as deviant despite the fact that they far exceed their own rules for elementary safety."*
>
> Diane Vaughan, author of The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA

Normalization of deviance occurs when a one-time deviation from initial thresholds does not result in a negative consequence (e.g., use of cell phones while driving). Participants rationalize the deviation with accepted practice and they generate a new set of expectations or new normal (normalization of the deviation); acceptance of the deviation continues until it becomes considered a (new) normal behavior. Eventually the team grows desensitized to the risk likelihood simply because it hasn't been realized yet. The process repeats until a failure occurs, either due to aggregation of the deviances, or simple statistics catches up.

In cases of long-term programs or hardware or software reuse, risks may not be identified for events familiar or common to the executing organization. From that organization's perspective, these new behaviors have been manageable under prior conditions, and any formal risk identification is deemed as unnecessary. In this syndrome, the accepted "norm" keeps getting adjusted (to higher risk) but there is never an aggregation of the adjusted risk.

To avoid this problem, analytical risk identification should be performed at program inception. Risk identification should consider the specific mission requirements, as well as prior problems, near-misses and work-arounds. Most importantly, the risk exposure must be periodically and independently reviewed.

4. Measure of Risk Identification Completeness

"We ignore the risks that are hardest to measure, even when they pose the greatest threats"

-The Signal and the Noise: Why So Many Predictions Fail – But Some Don't

By Nate Silver

Several distinct risk identification completeness measures exist, each with benefits and difficulties. Risk count is a high-level indicator that risk identification has been attempted. The Barrier Scorecard (Table 2) provides a means to assess the thoroughness of the risk ID process in presence of the likely barriers.

Table 2. Barrier Scorecard

Risk ID Area	Barrier Assessment Criteria	Assessment
Barrier 1: Over-Reliance on a Single Method	**1 The program uses only personal experience to identify risk.** **3 The program has access to many of the risk ID methods, but choice of method is at individual discretion.** **6 The program has access to many of the risk ID methods, and provides guidance on the appropriate usage.** **9 The program requires application of multiple risk ID methods.**	
Barrier 2: Artificial Constraints and Biases	**1 The program has explicitly established an artificial constraint or bias against complete risk identification.** **3 The program has implicit constraints and biases that limit, delay, or impede risk identification.** **6. There are minor constraints or biases which limit identification of minor risks, but significant risks are effectively identified.** **9 Risk identification process does not have constraints or biases to risk identification. The program actively challenges assumptions that may constrain risk identification.**	
Barrier 3: Dismissing a Risk as a Normal Program Challenge	**1 The program suppresses identification of risk for technical uncertainty.** **3 The program neither suppresses or encourages identification of risk for technical uncertainty.** **6 The program encourages risk identification of technical uncertainty.** **9 The program systematically and methodically reviews technical uncertainty and identifies associated risks.**	
Barrier 4: Compliance Reliance	**1 Program explicitly and formally assumes acceptable risk for compliant designs and processes.** **3 Compliant designs and processes are assumed to have no risk unless demonstrated otherwise.** **6 Program risk identifiers are encouraged to review design and process requirements and identify residual risks.** **9 Program employs systems engineering rigor including documentation of residual risks, rollup risks, and effects of lower level system performance to mission objectives.**	

Risk ID Area	Barrier Assessment Criteria	Assessment
Barrier 5: Program Acquisition Attributes	**1 Contract and program incentives actively constrain or bias effective risk identification.** **3 Program is encouraged to identify and mitigate contract incentives against effective risk identification.** **6 Contract type supports desired level of involvement in contractor's risk management process.** **9 Incentives in place for contractor to identify risks.**	
Barrier 6: Scope Boundaries	**1 Risk identification is explicitly restricted to within the boundaries of technical and/or contract scope.** **3 No prohibition against, or encouragement for identification of risk outside of technical and/or contract scope.** **6 Program elements are encouraged to identify risk at interfaces and at the integrated level.** **9 Programs implement specific processes for inter-element risk identification.**	
Barrier 7: Normalization of Deviance	**1 Program rejects or discourages identification of long-standing risks.** **3 Longstanding risks are identified if there is a change in assumption or criteria.** **6 Long standing risks are carried over to current programs.** **9 Program actively and systematically seeks to identify residual risks from heritage designs, processes, or assumptions.**	
Candidate Risks	**1 No formal repository for candidate risks; risks are captured in a risk list only after review and acceptance.** **3 Candidate risks are formally captured and reviewed. Unapproved candidate risks are closed.** **6 Streamlined process for formal capture of candidate risks to minimize investment until acceptance.** **9 Streamlined process for candidate risk ID, with periodic monitoring of unapproved risks until retired.**	

5. Recommendations

> *"When the facts change, I change my mind."*
> -John Maynard Keynes, Economist

The risk exposure of a program changes over time. Formalized risk identification employing multiple methods and forums should be repeated periodically, at program milestones, or when triggered by other indicators or changes.

Each recommendation is targeted at a particular function (customer, process, program, or industry forum), but the actual implementation of these recommendations may be tailored based on unique conditions. A combination of the recommended methods is needed to address the barriers identified. Table 3 summarizes the recommended actions for organizations to implement improved technical risk identification at program inception.

Table 3. Recommendations

ID	Recommendation	Barrier Mitigated							Function
		1	2	3	4	5	6	7	
1	Review list of risk identification methods and provide processes, tools, templates, and training to program risk managers.	X							Process
2	Plan to use several methods of risk identification at each program milestone and document it in the risk management plan (or equivalent).	X							Program
3	Require at least two risk identification methods for each program milestone or event, using at least one experiential method and one analytical method.	X							Program and Process
4	Risk ID template should include classification/grouping to aid in development of future guidance and checklists.	X	X					X	Process
5	Maintain a library of historical program risks, grouped by classification.	X	X	X	X				Process
6	Add risk identification as a discrete activity throughout the life cycle program milestones, design/readiness/peer reviews, of technical products (code reviews, modeling and simulation, rehearsals, and technical analyses), and phases (test and integration, launch).	X	X	X	X				Process and Program
7	Use change control forum, configuration management to evaluate and assumptions for potential changes to risk.	X		X	X				Program
8	Establish design review checklists that include identification of residual risks, assessment of modeling and simulation fidelity, and assessment of overall systems engineering quality. Use standard risk checklists to help ensure thoroughness. Programs with significant design heritage should carefully review the risks and anomalies identified by the legacy program. Inheritance reviews should be used to identify risks.	X			X	X		X	Process or Program
11	Implement risk identification as part of dispositioning nonconformances and anomalies. Specifically focus on unverified failures, 'accept as is' disposition, and failures in system integration and test.	X						X	Process
9	Monitor risk identification process for barriers and implementation of recommended solutions. This *independent* review should focus on the *process* and be separate from the review of risks.	X	X	X	X	X	X	X	Process and Customer
10	Develop a risk management community of practice to share common risks and best practices. This working group should include government and commercial customers, prime contractors, commercial space insurance brokers, and key technology suppliers.	X	X	X	X	X	X	X	Industry Forum
11	Normalize risks to a consistent level (e.g. unit and interface).		X						Program
12	Implement a metric or measure of risk identification completeness. Track progress, identify goals, and actively manage.		X						Process
13	Establish guidelines for filtering risks from issues. Create and maintain an issue tracking system that is effective in managing, planning, and mitigating the uncertain outcome of issues.		X						Process and Program
14	Encourage Risk ID by independent groups associated with the project such as customer and contractor functional organizations.		X	X			X	X	Process

ID	Recommendation	Barrier Mitigated							Function
		1	2	3	4	5	6	7	
15	Candidate risks should be processed prior to Risk Management review. Filtering may include screening, combining, interpreting, equalizing, and re-framing original ideas. This initial risk list has substantial value-added and is much more useful/actionable than raw list of candidate issues.		X		X			X	Program
16	Avoid focus on 'top N risks'. Plan periodic deep dive risk reviews to assess the entire list of identified risks including candidates and monitor risks. Pay special attention to TRL and heritage claims, NRE, areas with low margin, and other warning flags.		X			X			Customer
17	After ATP, revisit risk identification in collaborative forum. Avoid punitive response to risks not identified in RFP. Include inter-segment boundaries on contract scope margins.		X			X	X	X	Customer
18	Streamline process for candidate risks to minimize the investment in initial capture and review. If not accepted, candidate risks should be revisited periodically to assure that their state has not changed.		X					X	Process and Program
19	Streamline process for risk monitoring. Do not reject or close risks that have not been realized or completely mitigated, but require only periodic review.		X					X	Process
20	Link management reserve to risk and issue identification. Risks should be used to request MR and MR should be allocated to risks and issues.				X				Process
21	Analyze the sensitivities of system level performance to lower level performance and identify associated risks.					X			Program
22	Review RFP to encourage open review of risks. Encourage honest and open review of risks, and avoid penalizing identification of unanticipated risks.					X			Customer
23	Implement a supply chain technical risk identification program.						X	X	Process

Appendix A. Industry Review Results

The working group reviewed other industries to determine if there were significant differences in risk identification, and if these differences could be exploited in the government space industry. The industry research reinforced common risk identification practices and impacted some of the recommendations of this document. Specifically, the lessons for the space industry are:

- Classifying or grouping risk areas help in future risk identification efforts
- Checklists and databases are commonly accepted tools for risk identification
- Risk identification events should include multi-function representation
- Cognitive barriers exist and need recognition and time to overcome
- Industry working groups and communities of practice are valuable resources for risk identification

These lessons from other industries are included as appropriate in the Section 5 recommendations. The following paragraphs further elaborate the findings of this survey:

Auto Insurance Risk Identification

Auto insurance risk selection is the process by which vehicle insurers determine whom to insure and how much to charge. The system creates groupings of vehicles and driver actuarial classes based on the following classifications:

- Vehicle: Age; manufacturer, model; and value.
- Driver: Age; sex; marital status; driving record, violations; at fault accidents; and residence.
- Coverage type.
- Classifications, such as age, are further broken into actuarial classes, e.g., 21 to 24 year olds.

Supply Chain Risk Identification

There have been several attempts by supply chain managers to standardize risk identification. The team reviewed nine publications and found that there were several common themes:

- All recommended a structured approach to risk identification.
- Most recommended involving an independent perspective (audit, review, etc.).
- Most identified between five to nine risk categories.
- The more advanced solutions involved multi-stage risk identification (triage → detailed).
- Two studies focused on the interactive or compound risks; risks that depend on or are triggered by other risks.

Highway Transportation Risk Identification

Through internet search of reference documents, two documents stood out as significant:

1. *National Cooperative Highway Research Program (NCHRP) Report 658: Guidebook on Risk Analysis Tools and Management Practices to Control Transportation Project Costs*.
   Transportation Research Board of the National Academies; 2010
2. *Transportation Risk Management: International Practices for Program Development and Project Delivery*.
   Sponsored by: US Department of Transportation Federal Highway Administration; August 2012

These documents highlight several risk identification methods, their benefits, and their recommended application. They tended to divide the risks into recurring (common to many programs) and project specific.

Medical Industry Risk Identification

The medical industry focuses risk identification on patient health (conditions, detection, diagnoses, and treatments), patient rights, care/service delivery, and management. Generally they rely on standard risks (top 10), categories, and key metrics and indices.

Nuclear Reactor Safety Risk Identification

The Nuclear Regulatory Commission recommends a 'risk informed, performance based approach to regulating reactor safety'. This approach is focused primarily on three primary risk categories; core damage, radioactivity release, and injury to public and damage to environment.

Oil and Gas Industry Risk Identification

Oil and gas industry risk management relies heavily on independent expert assessment, and sorting by risk categories (financial, strategic, compliance, operations, and safety). They use event occurrence trending, process analysis, and use cross functional risk identification events.

Commercial Launch and Space Insurance Risk Identification

Commercial space insurance brokers and underwriters rely almost exclusively on comprehensive risk baselines and independent expert assessment. Total risk is monetized based on industry performance, prevailing market investment forces, and available capital. Mission specific technical risks identified by programs and independent reviewers are used to increment or decrement the premium. Reviewers use databases of historical failure rates for specific technologies, vendors, and contractors to identify risks. Only the top few risks have significant bearing on the premium, the remainder tends to be absorbed in the noise of other considerations. This approach is very useful to accurately predict returns on investments, but is not well suited to plan and execute specific technical mitigation. Adjustments to risk are typically achieved by changes in scope, liability, deductable values, criteria, and exclusions and not by mitigating specific risks.

US Government Intelligence Analysis Structured Analytic Techniques

This particular reference was recommended by one of the commercial space insurance brokers, and focuses on the cognitive barriers to identifying and correctly assessing diplomatic risks. It recommends several procedural methods to overcome cognitive barriers including diagnostic techniques, contrarian techniques, and imaginative thinking techniques. Most of this document is focused on the correct evaluation of risk, and not in risk identification. The few observations relating to risk identification are either specific to 'intelligence tradecraft' or are otherwise addressed in the methods described in Section 3.

Appendix B. Definition of Terms

There are many specific definitions for risk management terminology. We have established simple definitions as listed below to facilitate understanding of this document.

Term	Definition
Candidate Risk	An identified risk that has not been reviewed and accepted, rejected, identified to monitor, or retired.
Issue	A condition that exists or has already happened and has a negative consequence.
Monitor Risk	An active but acceptable risk not requiring active mitigation.
Program Inception	The preliminary phases of a program beginning at concept development, and proceeding through program baseline review.
Rejected Risk	A risk that has been reviewed and determined to be redundant to another risk, not credible, or does not result in a negative consequence.
Residual Risk	The level of risk after completion of all mitigation activities.
Retired Risk	A risk that no longer has any likelihood or consequence.
Risk	A future probable event that has a negative consequence.
Risk Analysis	The process of evaluating and measuring the likelihood and consequence of an identified risk, and the effect of planned and completed mitigation steps.
Risk Identification	The process of reviewing a program, product, or service for undesired potential results.
Risk List	A summary of managed risks.
Risk Management	A coordinated set of activities and methods used to assess, track, mitigate and measure risks on a program.
Risk Mitigation	Action(s) taken to reduce and/or eliminate the likelihood or consequence of a risk.
Risk Statement	A condition-consequence (if-then) statement that articulates a specific risk.

AEROSPACE REPORT NO.
TOR-2014-02201

Technical Risk Identification at Program Inception

Approved Electronically by:

Russell E. Averill, GENERAL MANAGER
SPACE BASED SURVEILLANCE DIVISION
SPACE PROGRAM OPERATIONS

Jacqueline M. Wyrwitzke, PRINC DIRECTOR
MISSION ASSURANCE SUBDIVISION
SYSTEMS ENGINEERING DIVISION
ENGINEERING & TECHNOLOGY GROUP

Rami R. Razouk, SR VP
ENG & TECH
ENGINEERING & TECHNOLOGY GROUP

Jackie M. Webb-Larkin, SECURITY SPECIALIST III
GOVERNMENT SECURITY
SECURITY OPERATIONS
OPERATIONS & SUPPORT GROUP

Technical Peer Review Performed by:

Norman Y. Lao, DIRECTOR DEPT
ACQ RISK & RELIABILITY ENGINEERING DEPT
MISSION ASSURANCE SUBDIVISION
ENGINEERING & TECHNOLOGY GROUP

Jacqueline M. Wyrwitzke, PRINC DIRECTOR
MISSION ASSURANCE SUBDIVISION
SYSTEMS ENGINEERING DIVISION
ENGINEERING & TECHNOLOGY GROUP

SK0675

External Distribution

REPORT TITLE		
Technical Risk Identification at Program Inception		
REPORT NO.	PUBLICATION DATE	SECURITY CLASSIFICATION
TOR-2014-02201	April 20, 2014	UNCLASSIFIED

Charles Abernethy
Aerojet
charles.abernethy@aerojet.com

Scott Anderson
Seaker
scott.anderson@seaker.com

Ken Baier
Lockheed Martin
ken.b.baier@lmco.com

Carlo Abesamis
NASA
abesamis@jpl.nasa.gov

Aaron Apruzzese
ATK
aaron.apruzzese@atk.com

Dean Baker
NRO
bakerdea@nro.mil

Andrew Adams
Boeing
andrew.c.adams@boeing.com

Chic Arey
NRO
areyc@nro.mil

Mark Baldwin
Raytheon
Mark.L.Baldwin@raytheon.com

David Adcock
Orbital
adcock.david@orbital.com

Brent Armand
Orbital
Armand.Brent@orbital.com

Lisa Barboza
General Dynamics
Lisa.Barboza@gd-ais.com

Robert Adkisson
Boeing
robert.w.adkisson@boeing.com

Larry Arnett
Loral
arnett.larry@ssd.loral.com

Glenn Barney
Comdev-USA
glenn.barney@comdex-use.com

David Beckwith
NRO
beckwith@nro.mil

Christopher Brust
DCMA
Christopher.Brust@dcma.mil

Will Caven
Loral
caven.will@ssd.loral.com

Theresa Beech
Metispace
tbeech@metispace.com

Alexis Burkevics
Rocket
Alexis.Burkevics@rocket.com

Shawn Cheadle
Lockheed Martin
shawn.cheadle@lmco.com

Barry Birdsong
MDA
barry.birdsong@mda.mil

Thomas Burns
NOAA
thomas.burns@noaa.gov

Janica Cheney
ATK
janica.cheney@atk.com

Ruth Bishop
Northrop Grumman
ruth.bishop@ngc.com

Edward Bush
Northrop Grumman
Edward.Bush@ngs.com

Brian Class
Orbital
class.brian@orbital.com

Robert Bodemuller
Ball
rbodemuller@ball.com

Tim Cahill
Lockheed Martin
tim.cahil@lmco.com

Brad Clevenger
EMCORE
brad_clevenger@emcore.com

Silvia Bouchard
Northrop Grumman
silver.bouchard@ngc.com

Kevin Campbell
Exelis Inc
kevin.campbell@exelisinc.com

Jerald Cogen
FREQELEC
Jerald.Cogen@FreqElec.com

Wayne Brown
ULA Launch
wayne.brown@ulalaunch.com

Larry Capots
Lockheed Martin
larry.capots@lmco.com

Bernie Collins
DNI
bernie.f.collins@dni.gov

Jeff Conyers
Ball
jconyers@ball.com

Douglas Dawson
NASA
douglas.e.dawson@jpl.nasa.gov

David Eckhardt
BAE Systems
david.g.eckhardt@baesystems.com

Kevin Crackel
Aerojet
kevin.crackel@aerojet.com

Jaclyn Decker
Orbital
decker.jaclun@orbital.com

Robert Ellsworth
Boeing
robert.h.ellsworth@boeing.com

James Creiman
Northrup Grumman
James.Creiman@ngc.com

Larry DeFillipo
Orbital
defillipo.aryy@orbital.com

Matt Fahl
Harris Corporation
mfahl@harris.com

Stephen Cross
ULA Launch
stephen.d.cross@ulalaunch.com

Ken Dodson
SSL MDA
ken.dodson@sslmda.com

James Farrell
Boeing
james.t.farrell@boeing.com

Shawn Cullen
JDSU
shawn.cullen@jdsu.com

Tom Donehue
ATK
tom.donehue@atk.com

Tracy Fiedler
Raytheon
tracy.m.fiedler@raytheon.com

Louis D'Angelo
Lockheed Martin
louis.a.d'angelo@lmco.com

Mary D'Ordine
Ball
mdordine@ball.com

Brad Fields
Orbital
fields.brad@orbital.com

David Davis
SMC
David.Davis.3@us.af.mil

Susanne Dubois
Northrop Grumman
susanne.dubois@ngc.com

Sherri Fike
Ball
sfike@ball.com

Richard Fink
NRO
richard.fink@nro.mil

Matteo Genna
SSL
matteo.genna@sslmda.com

Joe Haman
Ball
jhaman@ball.com

Bruce Flanick
Northrop Grumman
bruce.flanick@ngc.com

Helen Gjerde
Lockheed Martin
helen.gjerde@lmco.con

Lilian Hanna
Boeing
lilian.hanna@boeing.com

Mike Floyd
General Dynamics
Mike.Floyd@gdc4s.com

Ricardo Gonzalez
BAE Systems
ricardo.gonzalez@baesystems.com

Harold Harder
Boeing
harold.m.harder@boeing.com

David Ford
Flextronics
david.ford@flextronics.com

Dale Gordon
Rocket
dale.gordon@rocket.com

Bob Harr
Seaker
bob.harr@seaker.com

Robert Frankievich
Lockheed Martin
robert.h.frankievich@lmco.com

Chuck Gray
Fescorp
Chuckg@fescorp.com

Frederick Hawthorne
Lockheed Martin
frederick.d.hawthorne@lmco.com

Bill Frazier
Ball
wfrazier@ball.com

Luigi Greco
Exelis Inc
luigi.greco@exelisinc.com

Ben Hoang
Orbital
Hoang.Ben@orbital.com

Jace Gardner
Ball
jgardner@ball.com

Gregory Hafner
Orbital
Hafner.Gregory@orbital.com

Rosemary Hobart
Hobart Machined
rosemary@hobartmachined.com

Richard Hodges
NASA
richard.e.hodges@jpl.nasa.gov

Amanda Johnson
Orbital
johnson.amanda@orbital.com

Mark King
Micopac
markking@micropac.com

Paul Hopkins
Lockheed Martin
paul.c.hopkins@lmco.com

Edward Jopson
Northrop Grumman
edward.jopson@ngc.com

Andrew King
Boeing
andrew.m.king@boeing.com

Kevin Horgan
NASA
kevin.horgan@nasa.gov

Jim Judd
orbital
judd.jim@orbital.com

Byron Knight
NRO
knightby@nro.mil

Eugene Jaramillo
Raytheon
eugenejaramillo@raytheon.com

Geoffrey Kaczynski
NEA Electronics
gkazynik@neaelectonics.com

Hans Koenigsmann
SpaceX
hans.koenigsmann@spacex.com

Dan Jarmel
Northrop Grumman
dan.jarmel@ngc.com

Mike Kahler
Ball
mkahler@ball.com

James Koory
Rocket
james.koory@rocket.com

Robert Jennings
Raytheon
rjennings@raytheon.com

Yehwan Kim
Moog
ykim@moog.com

Brian Kosinski
SSL
Kosinski.Brian@ssd.loral.com

Mike Jensen
ULA Launch
mike.jensen@ulalaunch.com

Jeff Kincaid
Power
Jeffrey.Kincaid@pwr.utc.com

John Kowalchik
Lockheed Martin
john.j.kowalchik@lmco.com

Rick Krause
Ball
rkrause@ball.com

Eric Lau
SSL
lau.eric@ssd.loral.com

Henry Livingston
BAE Systems
henry.c.livingson@baesystems.com

Steve Krein
ATK
steve.krein@atk.com

Marvin LeBlanc
NOAA
Marvin.LeBlanc@noaa.gov

Art Lofton
Northrop Grumman
Art.Lofton@ngc.com

Steve Kuritz
Northrop Grumman
steve.kuritz@ngc.com

Scott Lee
Northrop Grumman
Scott.lee@ngc.com

James Loman
SSL
james.loman@sslmda.com

Louise Ladow
Seaker
louise.ladow@seaker.com

Don LeRoy
Barden Bearings
dleroy@bardenbearings.com

Jim Loman
SSL
loman.james@ssd.loral.com

C J Land
Harris
cland@harris.com

Scot Lichty
Lockheed Martin
scot.r.lichty@lmco.com

Lester Lopez
Harris
llopez04@harris.com

Chris Larocca
EMCORE
clarocca@emcore.com

Sultan Ali Lilani
Integra - Tech
sultan.lilani@integra-tech.com

Frank Lucca
1-3 Com
frank.l.lucca@1-3com.com

Robert Lasky
Orbital
lasky.robert@orbital.com

Josh Lindley
MDA
joshua.lindley@mda.mil

Joan Lum
Boeing
joan.l.lum@boeing.com

Brian Mack
Orbital
mack.brian@orbital.com

Jeff Mendenhall
MIT
mendenhall@ll.mit.edu

Deanna Musil
SSL
deanna.musil@sslmda.com

Julio Malaga
Orbital
malaga.julio@orbital.com

Jo Merritt
AVTEC
jmerritt@avtec.com

Thomas Musselman
Boeing
thomas.e.musselman@boeing.com

Kevin Mallon
1-3 Com
Kevin.P.Mallon@1-3com.com

Charles Mills
Lockheed Martin
charles.a.mills@lmco.com

John Nelson
Lockheed Martin
john.d.nelson@lmco.com

Miroslav Maramica
Area 51
miroslav@area51esq.com

Edmond Mitchell
APL
edmond.mitchell@jhuapl.edu

Dave Novotney
EBA
dbnovotney@eba-d.com

John Mc Bride
Orbital
Mcbride.John@orbital.com

Dennis Mlynarski
Lockheed Martin
dennis.mlynarski@lmco.com

Ron Nowlin
EaglePicher
ron.nowlin@eaglepicher.com

Ian McDonald
BAE Systems
ian.a.mcdonald@baesystems.com

George Mock
NYE Lubricants
gbm3@nyelubricants.com

Mike Numberger
Navy
nurnberger@nrl.navy.mil

Kurt Meister
Honeywell
kurt.meister@honeywell.com

Nancy Murray
Safety Batteries
Nancy.murray@saftbatteries.com

Michael O'Brien
Exelis Inc
michael.obrien@exelisinc.com

Michael Ogneovski
Exelis Inc
michael.ognenovski@exelisinc.com

Paulette Megan
Orbital
paulette.megan@orbital.com

David Rea
BAE Systems
david.a.rea@baesystems.com

Debra Olejniczak
Northrop Grumman
Debra.Olejniczak@ngc.com

Mark Pazder
Moog
mpazder@moog.com

Forrest Reed
EaglePicher
forrest.reed@eaglepicher.com

Larry Ostendorf
psemc
Lostendorf@psemc.com

Steven Pereira
APL
Steven.Pereira@jhuapl.edu

Thomas Reinsel
Raytheon
thomas_j_reinsel@raytheon.com

Anthony Owens
Raytheon
anthony_owens@raytheon.com

Richard Pfisterer
APL
Richard.Pfisterer@jhuapl.edu

Bob Ricco
Northrop Grumman
bob.ricco@ngc.com

Joseph Packard
Exelis Inc
Joseph.packard@exelisinc.com

Angela Phillips
Raytheon
amphillips@raytheon.com

Mike Rice
RT Logic
mrice@rtlogic.com

Peter Pallin
SSL
peter.pallin@sslmda.com

Dave Pinkley
Ball
dpinkley@ball.com

Sally Richardson
Orbital
richardson.sally@orbital.com

Richard Patrican
Raytheon
Richard.A.Patrican@raytheon.com

Kay Rand
Northrop Grumman
kay.rand@ngc.com

Troy Rodriquez
Sierra Microwave
troy_rodriquez@sierramicrowave.com

Ralph Roe
NASA
ralph.r.roe@nasa.gov

Michael Sampson
NASA
michael.j.sampson@nasa.gov

Michael Settember
NASA
michael.a.settember@jpl.nasa.gov

Mike Roller
UTAS
mike.roller@utas.utc.com

Victor Sank
NASA
victor.j.sank@nasa.gov

Tom Sharpe
SMT Corp
tsharpe@smtcorp.com

John Rotondo
Boeing
john.l.rotondo@boeing.com

Don Sawyer
AVNET
don.sawyer@avnet.com

Jonathan Sheffield
SSL
jonathan.sheffield@sslmda.com

William Rozea
Rocket
william.rozea@rocket.com

Fred Schipp
MDA - Navy
frederick.schipp@navy.mil

Andrew Shroyer
Ball
ashroyer@ball.com

Dennis Rubien
Northrop Grumman
dennis.rubien@ngc.com

Jim Schultz
Boeing
james.w.schultz@boeing.com

Fredic Silverman
HSTC
fsilverman@hstc.com

Larry Rubin
SSL
Rubin.larry@ssd.loral.com

Gerald Schumann
NASA
gerald.d.schumann@nasa.gov

Rob Singh
SSL
rob.singh@sslmda.com

Lane Saechao
Rocket
lane.saechao@rocket.com

Annie Sennet
Safety Batteries
Annie.Sennet@saftbarries.com

Kevin Sink
TTINC
kevin.sink@ttinc.com

Melanie Sloane
Lockheed Martin
melanie.sloane@lmco.com

David Swanson
Orbital
swanson.david@orbital.com

Marvin VanderWeg
SpaceX
marvin.vanderwag@spacex.com

Jerry Sobetski
Lockheed Martin
jerome.f.sobetski@lmco.com

Mauricio Tapia
Oribital
tapia.mauricio@orbital.com

Gerrit VanOmmering
SSL
gerrit.vanommering@sslmda.com

LaKeisha Souter
Northrop Grumman
lakeisha.souter@ngc.com

Jeffrey Tate
Raytheon
jeffery_tate@raytheon.com

Michael Verzuh
Ball
mverzuh@ball.com

Jerry Spindler
Execlis Inc
Jerry.Spindler@exelisinc.com

Bill Toth
Northrop Grumman
william.toth@ngc.com

John Vilja
Power UTC
jussi.vilja@pwr.utc.com

Peter Stoltz
TX Corp
pstoltz@txcorp.com

Ghislain Turgeon
SSL
ghislain.turgeon@sslmda.com

Vinvent Stefan
Orbital
vincent.stefan@orbital.com

Thomas Stout
Northrop Grumman
thomas.stout@ngc.com

Deborah Valley
MIT
deborah.valley@ll.mit.edu

James Wade
Raytheon
james.w.wade@raytheon.com

George Styk
Exelis Inc
george.styk@exelisinc.com

Fred Van Milligen
JDSU
fvanmilligen@jdsu.com

John Walker
SSL
JohnF.Walker@sslmda.com

Brian Weir
Booz Allen Hamilton
weir_brian@bah.com

Larry Wray
SSL
wray.larry@ssd.loral.com

Arthur Weiss
Power UTC
arthur.weiss@pwr.utc.com

Mark Wroth
Northrop Grumman
mark.wroth@ngc.com

Craig Wesser
Norhtrop Grumman
craig.wesser@ngc.com

Jian Xu
Aeroflex
jian.xu@aeroflex.com

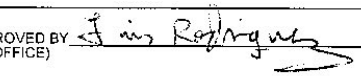
Dan White
Comdex-USA
dan.white@comdev-usa.com

George Young
Raytheon
gyoung@raytheon.com

Thomas Whitmeyer
NASA
tom.whitmeyer@nasa.gov

Charlie Whitmeyer
Orbital
whitmeyer.charlie@orbtial.co
m

Michael Woo
Raytheon
michael.woo@raytheon.com

APPROVED BY (AF OFFICE)  DATE June 30, 2014