U.S. DEPARTMENT OF COMMERCE
Office of Inspector General

Office of the Secretary

Top Management Challenges Facing the Department of Commerce

Final Report No. OIG-19384
November 2008

FOR PUBLIC RELEASE

Office of Audit and Evaluation

UNITED STATES DEPARTMENT OF COMMERCE
Office of Inspector General
Washington, D.C. 20230

November 18, 2008

MEMORANDUM FOR THE SECRETARY

Todd J. Zinser

FROM: Todd J. Zinser

SUBJECT: Top Management Challenges Facing the Department

The Office of Inspector General (OIG) is required by statute to annually report the top management challenges facing the Department of Commerce. We regularly discuss the Department's progress in addressing these challenges in the *IG's Semiannual Report to Congress* and the Department's *Performance and Accountability Report.* We prepared this year's report to highlight the top management challenges for the incoming leadership at the Department as part of the Presidential transition.

In our view, there are five critical issues the new Secretary and senior management team will need to focus immediate and considerable attention on, and we detail them, as follows, in this report:

1) Overcome the setbacks experienced in reengineering decennial processes, and conduct a successful 2010 Census.

2) Better position the Department to address information security risks.

3) Effectively manage the development and acquisition of NOAA's two environmental satellites.

4) Establish a safety culture at NIST.

5) Ensure NTIA effectively carries out its responsibilities under the Digital Television Transition and Public Safety Act.

OFFICE OF INSPECTOR GENERAL
OIG
U.S. DEPARTMENT OF COMMERCE

We also discuss several other areas that pose distinct challenges to the Department's mission success and will therefore require the Secretary's sustained attention:

- Weaknesses in the Department's acquisition oversight and acquisition workforce
- USPTO's long and growing patent processing times, and its financing vulnerabilities
- NOAA's ability to conserve the nation's fragile oceans and living marine resources while ensuring a vital U.S. commercial fishing industry
- BIS' setbacks in modernizing its obsolete information technology infrastructure to strengthen the dual-use export control system

The challenges identified in our report reflect the broad findings of our work throughout the Department and the observations made by secretarial officers and heads of operating units during recent discussions with them. Two recurring themes emerged during these discussions, which serve as useful background for the new leadership in approaching the top challenges: (1) leading the Department's autonomous bureaus, with their entrenched cultures that resist change, is exceedingly difficult, and (2) Commerce must deal with substantial infrastructure needs—such as upgrading aging IT assets and improving IT security—in a constrained budget environment.

Autonomous Bureaus with Entrenched Cultures. The historical mission of the Department is "to foster, promote, and develop the foreign and domestic commerce" of the United States. As a result of legislative and administrative additions, this mission now broadly encompasses the responsibility to foster, serve, and promote the nation's economic development and technological advancement, and the activities of 12 disparate operating units. The Secretary's principal focus is on formulating policy and providing advice to the President on this mission, particularly as it impacts U.S. trade activities and promotion. But Commerce leadership must also ensure effective administrative processes (e.g., financial, human resources, procurement, information technology) Department-wide in order to carry out program operations.

The Department has been characterized as a holding company of 12 autonomous bureaus, most of which have long-established business models. The bureaus resist the centralized direction, control, and oversight needed to ensure that administrative processes are consistently and effectively applied. This autonomy is a substantial impediment to departmental efforts to control and improve these processes. Nevertheless, the Secretary is ultimately responsible for the performance of the Department as a whole, and needs to be able to effect program and process improvements and hold the bureaus accountable for their performance. To do so effectively requires establishing a shared vision among bureau leadership who in turn must marshal the cooperation of the Department's career workforce.

Commerce's career workforce is knowledgeable, long serving, and dedicated to the Department's mission. The countless benefits of having such a workforce need no explanation. But these characteristics also mire the bureaus in entrenched cultures that are resistant to change. In this past year alone, there have been two prime examples in which a bureau's culture contributed to significant problems—the failure of Census's plan to use handheld computers for nonresponse follow-up in the 2010 decennial census and the plutonium spill at the National Institute of Standards and Technology's Boulder campus.

An overarching challenge for the new Secretary and leadership team will be to break down the cultural barriers that impede cohesive and effective Department-wide management.

Infrastructure Needs. The government is operating in an era of constrained budgets, requiring federal agencies to address critical infrastructure needs, such as IT security and aging IT systems, with limited existing resources. At Commerce this practice is quickly becoming unsustainable. The many critical infrastructure needs of the Department can no longer be funded with existing resources without significantly impacting essential, mission-related activities. The Department will have to develop convincing business cases to obtain the resources to address critical IT security and infrastructure needs and effectively manage these resources.

We appreciate the courtesies you, the Deputy Secretary, and other secretarial officers and heads of operating units extended to us during our recent meetings to discuss the management challenges.

If you have any questions concerning this report, please contact me at (202) 482-4661. You may also contact Judith J. Gordon, assistant inspector general for audit and evaluation, at (202) 482-2754.

Contents

1. Overcome the Setbacks Experienced in Reengineering Decennial Processes, and Conduct a Successful 2010 Census

The ability of the U.S. Census Bureau to successfully conduct its constitutionally mandated decennial count of U.S. residents in 2010 is at serious risk. After spending 8 years developing a completely new approach to census-taking—one that was to automate major field operations—the bureau scrapped plans for using handheld computer technology for the largest and most expensive of these operations, known as nonresponse follow-up, because of significant performance problems and the bureau's loss of confidence in the Field Data Collection Automation (FDCA) contractor. It will now conduct this operation using paper and pencil, as it has done in previous censuses. The inability of Census and its contractor to work together to produce a handheld computer and related systems for field data collection as originally envisioned, combined with major flaws in the bureau's cost-estimating methods and other issues, have added an estimated $2.2 billion to $3 billion to the original $11.5 billion life-cycle cost estimate for the 2010 decennial.

The Department and the Census Bureau have taken significant actions during the past year to address problems. These actions include extensive changes to decennial management, improvements in program management practices, and closer oversight of the decennial effort by the Department. However, despite these changes, significant risks remain for the 2010 decennial. Whether the bureau can retool in time to conduct a reliable census, even at this increased price tag, represents, in our view, the most significant challenge facing the new Secretary of Commerce.

Census 2010 was to be the first high-tech count in the nation's history, with decennial employees using handheld computers to verify addresses through global-positioning software, collect data from households that did not mail back census questionnaires (i.e., nonresponse follow-up), and manage a variety of information and tasks. The handheld computers were the centerpiece of the strategy and other decennial operations were built around or impacted by the decision to use them. Now nonresponse follow-up will revert to the traditional paper and pencil operation it has always been. The switch to paper processes will require additional field staff and support personnel—which means more time to hire and train, and more dollars to do so. And it means Census must modify its other plans and operations to account for the change.

Continued problems related to the FDCA project and the late transition to paper-based processes without extensive testing create an unprecedented level of risk. An inaccurate population count will have unacceptable consequences for the nation: at stake is apportionment of the 435 seats in the House of Representatives and equitable distribution of billions of dollars in federal and state aid. Both GAO and OMB have designated the 2010 census as a high-risk program and it is under intense scrutiny by Congress.

Program and contract mismanagement caused significant problems

The overarching explanation for the significant problems Census has encountered to date is the failure of senior Census Bureau managers in place at the time to anticipate the complex IT requirements involved in automating the census. We reported numerous problems in the development and acquisition of the handheld devices and related field automation earlier in the decade. Census had originally intended to develop the handhelds in-house and tested prototypes in both 2004 and 2006. The devices had serious problems in both tests. These experiences should have better informed the bureau's efforts to define requirements.

The bureau decided too late in the decade to contract for automation of field operations to meet ambitious fixed deadlines for the dress rehearsal tests starting in 2007 and decennial operations starting in 2009. After contract award, the bureau's requirements remained in flux. As late as January 2008—nearly 2 years after contract award—Census finally delivered a first draft of a complete, user-validated set of requirements for the handhelds and supporting infrastructure. It had no contingency plan in the event the handhelds proved unusable.

The problems experienced in developing the handhelds have led to tremendous setbacks for numerous operations in addition to nonresponse follow-up: plans for testing and enhancing the handhelds for address canvassing—the only operation that will still use the devices—have been severely compressed. Address canvassing will undergo its final operational test over an 8-day period, rather than the 3 months originally allotted in the plan for the retooled census. This operation is essential to, among other things, successfully delivering questionnaires and giving temporary staff accurate addresses and maps for nonresponse follow-up. Dress rehearsal testing of the operation—which concluded in June 2007—revealed serious technical problems. We question whether Census will have the time to resolve issues arising from the 8-day test, scheduled for December, before the start of the 2010 operation. Training of address canvassers for the live operation commences in February 2009, leaving the bureau only a short period of time to fix any problems identified in this final test.

Help desk operations—key to ensuring the handhelds function properly during address canvassing—are just now in the process of being redesigned. Census is also taking over the regional census center communications infrastructure, which under the contractor has experienced numerous problems that must be resolved to ensure a successful 2010 count.

Meanwhile, because of the inordinate attention and resources necessary to address field automation problems, Census has been unable to address the readiness of operations for enumerating some traditionally difficult groups and settings, such as the homeless, military bases, and group quarters—it dropped plans to test these operations from the 2008 dress rehearsal, which means the actual decennial count will be the proving ground for these operations. Enumeration procedures it previously tested—such as those planned for American Indian reservations—showed almost no effect on mitigating long-standing obstacles to producing an accurate count. Yet the bureau has had no time to develop and test possible improvements.

Finally, the bureau must have a fingerprinting program in place prior to hiring the estimated 1.3 million temporary workers needed for field operations. Because the decision to fingerprint was made only recently, Census faces significant risks in implementing this estimated $148 million operation.

Organizational culture contributed to problems

The Census Bureau—particularly headquarters—is an insular organization that eschews open dialog with outside parties and even its own regional operations. As decennial census planning proceeded, the bureau minimized the significance of its problems, withheld information, and was not forthcoming with the Department, Congress, OIG, and other oversight agencies about the problems it was experiencing. Perhaps the most egregious example of the bureau's insularity was its lack of transparency about the FDCA problems, allowing them to persist to the point of crisis. It was not until January 2, 2008, after a news report in *Government Executive* of a leaked MITRE analysis raising numerous red flags, that the Department, OMB, Congress, and other stakeholders became aware of the dire condition of the program. Presented to the then-deputy Census director in late November 2007, the MITRE document concluded,

> FDCA is in serious trouble. It is not clear the system will meet Census' operational needs and quality goals. The final cost is unpredictable. Immediate, significant changes are required to rescue the program. However, the risks

> are so large considering the available time that we recommend immediate development of contingency plans to revert to paper operations.

This was not MITRE's first warning. It had briefed the deputy director about the FDCA problems in June 2007. When this briefing appeared to stimulate little action, MITRE prepared the November analysis. Less than 2 weeks after the November warning, the then-bureau director testified to Congress that the handheld computer was working well, and gave no indication of MITRE's concerns.

In the wake of the FDCA problems, the Secretary of Commerce announced that management and oversight of the 2010 census would be strengthened and deepened both at the bureau and the Department. He assigned several members of the Department's senior political leadership to work with the bureau on a recovery plan, which has given the Secretary some measure of influence over the plan and visibility into the bureau's progress. The upcoming transition of key departmental leadership positions necessarily creates the risk of disrupting existing oversight efforts for the most critical program for which the new Secretary will initially be accountable.

The Census Bureau prides itself on its "can do" attitude and considers tenure through multiple decennial censuses a prerequisite for any senior decennial position. Bureau staff views the decennial as so unique that there is little to be learned from newcomers or external sources no matter how distinguished or knowledgeable.

This vision has left the bureau generally unreceptive to new ways of doing business. It has not kept pace with private sector advances in business process improvement and lacks insight into how these advances can benefit census operations. In deciding to use handhelds for decennial field automation—viewed by the bureau as a huge operational transformation—the bureau showed little regard or appreciation for the time and effort involved in gaining buy-in for significant business process changes from Census staff.

Leadership with private sector expertise is vital not only for improving decennial management but also for reappraising the bureau's other programs and administrative operations. Although the bureau made personnel changes after the FDCA crisis became public, it has not yet brought in external management with expertise in successfully running complex programs and system acquisitions or in implementing contemporary private sector management methods. Both we and outside experts recommend such experience as a necessary requirement for shoring up the bureau's management weaknesses and combating its insularity. Since the Census director is a Presidential appointee, there is the prospect that the director position will turn over again after the current director has been on the job for slightly more than 1 year. The inevitable delay involved in nominating and gaining confirmation of a new director means that the bureau will begin major decennial operations without the benefit of significant leadership continuity and management improvements. Given the major late-stage changes to 2010 operations, having two short-time directors during the final 2 years of the decennial cycle, coupled with the long-term absence of proven high-level management expertise, could create additional challenges the bureau must be poised to address.

With the first major decennial operation (address canvassing) beginning in early 2009, the new Secretary will have little opportunity to impact planning for the 2010 decennial, although he or she will have responsibility for its overall implementation. The new Secretary *does* have the opportunity to impact planning for the 2020 census. We believe that applying the lessons learned from the 2010 decennial to the planning and reengineering of the 2020 decennial should also be a high priority for the new Secretary.

For more information, view the documents below at www.oig.doc.gov:

Reports

- 2010 Decennial Census: Dress Rehearsal of Address Canvassing Revealed Persistent Deficiencies in Approach to Updating the Master Address File (OSE-18599, October 2008)
- 2010 Decennial Census: Census Should Further Refine Its Cost Estimate for Fingerprinting Temporary Staff (OIG-19058-1, August 2008)
- 2010 Decennial Census: OIG Reviews Through the Decade Identify Significant Problems in Key Operations (OIG-19217, June 2008)
- 2010 Census: Key Challenges to Enumerating American Indian Reservations Unresolved by 2006 Census Test (OSE-18027, September 2007)
- Enumerating Group Quarters Continues to Pose Challenges (IPE-18046, October 2006)
- Valuable Learning Opportunities Were Missed in the 2006 Test of Address Canvassing (OIG-17524, March 2006)

In-Progress Reviews

- Audit of the Field Data Collection Automation Contract Type and Award Fee
- OIG Reviews of Decennial Census in Response to Secretarial Request

2. Better Position the Department to Address Information Security Risks

As in many federal agencies, putting proper information security controls in place has been an intractable problem at the Department of Commerce and a long-standing item on OIG's watch list. Despite additional expenditures to mitigate the problem, the Department has reported information security as a material weakness every year since FY 2001.

What Is Certification & Accreditation and Why Is It Important?

Certification is a comprehensive assessment of security controls implemented in a computer system. It determines whether controls are implemented correctly, operating as intended, and meeting the security requirements for the system. Through the formal assessment of controls, the certifier identifies any vulnerabilities that have not been eliminated.

Accreditation is management's formal authorization to allow a system to operate and its explicit acceptance of the risks posed by remaining vulnerabilities. Through accreditation, senior agency officials take responsibility for the security of systems they manage and for any adverse impacts should a breach in security occur.

The Federal Information Security Management Act (FISMA) requires agencies to certify that their systems and data are protected with adequate, functioning security controls before authorizing (accrediting) a system to operate. The reason for the material weakness at Commerce has been consistently inadequate certification and accreditation (C&A): year after year our FISMA reviews have found ineffective C&A processes that do not adequately identify and assess needed controls and ultimately fail to assure that systems and data are protected.

Securing systems from cyber threats is clearly the most difficult piece of the challenge, because these threats represent a moving target: they increase in number and sophistication almost daily. And as agencies incorporate wireless and other technologies to support their operations and workplace flexibilities, they invite new risks that must be anticipated and mitigated.

To be effective in this environment, the Department's IT security program must be proactive and fluid, staffed by IT security professionals who have the appropriate skills and experience to implement required security controls, assess their effectiveness, and anticipate and respond to emerging threats. They also need appropriate security clearances to effectively deal with potential cyber attacks by hackers, terrorist groups, organized crime, and nation-states. We have found IT security personnel lack adequate understanding of the Department's IT security policy, NIST standards and guidance, and security technology, and therefore cannot appropriately apply them. The Department cites lack of resources as a major impediment to improving IT security.

Commerce has had some notable security incidents that underscore the potential for harm.

- The Bureau of Industry and Security, which processes sensitive export license data, took one of its information systems off line in late 2006, after discovering it had been hacked, and the agency still has only limited Internet access. BIS reported that it reviewed firewall logs for the 8 months prior to detecting the intrusion, but could not determine how long the hackers were inside the system before their presence was discovered.

- The Census Bureau was one of several federal agencies to report hundreds of lost laptops potentially containing sensitive data. We assessed whether the laptops had adequate security controls to prevent unauthorized access. We determined they did not, and in fact could be compromised with tools that were readily available on the Internet. Census has since implemented full-disk encryption on its laptops to protect sensitive information.

- This past spring, U.S. authorities investigated media reports that a Commerce Department laptop carried on a foreign visit had been compromised and whether hackers could have obtained information to enable them to penetrate Commerce systems. Though the incident was not substantiated, the concern of wider access to Commerce systems reflects the core purpose and importance of effective C&A coupled with a dynamic IT security program: together they ensure controls to prevent such wider access are in place and constantly upgraded to mitigate new threats.

Joint OIG-Department plan, with focus on continuous monitoring of security controls, is improving Commerce's security status

We have been working with the Department to eliminate the material weakness by the end of 2009 under a jointly developed plan that incorporates realistic milestones and measurable steps for building consistent and repeatable C&A practices. A key element of the strategy is continuous monitoring of security controls. The National Institute of Standards and Technology is updating its FISMA guidance to give greater emphasis to continuous monitoring as part of C&A. Continuous monitoring requires agencies to regularly assess and adjust their security controls to maintain or improve protective measures on an ongoing basis.

Our FY 2008 FISMA reviews noted improvements: we looked at nine systems and concluded that four of them (44 percent) were operating in compliance with federal and Department requirements (compared with 33 percent in FY 2007). Only one of the four had used an acceptable C&A process at the time of our review, but the remaining three showed subsequent improvements because of rigorous continuous monitoring activities.

Our FY 2008 FISMA review also looked at two USPTO systems—one operated by the agency and one operated by a contractor. USPTO, which reports on its performance separately from the Department, first reported a material weakness in information security in FY 2002 because of inadequate C&A. With the exception of FY 2004 and FY 2005, USPTO has continued to report the material weakness. Both of the systems we looked at this year had deficient security plans, configuration settings, and security control assessments. Therefore, we concluded the IT security material weakness remains.

USPTO has initiated an effort to improve its C&As by having them verified and validated by an independent party before making the authorization decision. Also, USPTO has implemented a process to better document security control assessments and results, and continues to develop and refine a set of common security controls applicable to all of its systems. We therefore expect to see improvements in the future.

Cyber Security Management and Assessment Tool should strengthen continuous monitoring efforts

The Department has made progress toward implementing the Cyber Security Assessment and Management (CSAM) tool—a software application developed by the Department of Justice that allows users to take a 360-degree approach to C&A—they can input system information as they begin the C&A process, and, among other things, generate and implement a security plan that complies with FISMA requirements, analyze security requirements, and track resolution of vulnerabilities and the results of security control monitoring. The systems we reviewed this year were certified and accredited without the benefit of the tool. But once fully integrated, the tool should bring greater consistency to the C&A process across all Commerce bureaus, including USPTO, and give management greater visibility into it.

For more information, view the documents below at www.oig.doc.gov:

Reports

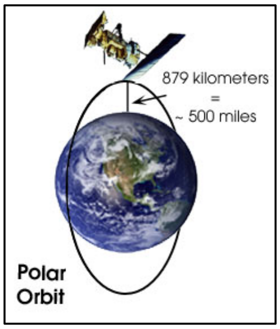
- FY 2008 FISMA Assessment of NWS Telecommunication Gateway System (OSE-19000, September 2008)
- FY 2008 FISMA Assessment of BEA Estimation Information Technology System (OSE-19001, September 2008)
- FY 2008 FISMA Assessment of Census Wireless Data Communications General Support System (OSE-19163, September 2008)
- FY 2008 FISMA Assessment of Field Data Collection Automation System (OSE-19164, September 2008)
- FY 2008 FISMA Assessment of NMFS Science and Technology System (OSE-19165, September 2008)
- FY 2008 FISMA Assessment of NWS International Satellite Communications System (OSE-19166, September 2008)
- FY 2008 FISMA Assessment of NESDIS Satellite Environmental Processing System (OSE-19167, September 2008)
- FY 2008 FISMA Assessment of Landon IP Information System (OSE-19367, September 2008)
- FY 2008 FISMA Assessment of Enterprise Remote Access System (OSE-19368, September 2008)
- FY 2007 FISMA Assessment of the Network Operations Center (OSE-18688, September 2007)
- FY 2007 FISMA Assessment of Client Services General Support System (OSE-18690-1, September 2007)
- FY 2007 FISMA Assessment of AESDirect Major Application (OSE-18690-2, September 2007)
- FY 2007 FISMA Assessment of Core Network General Support System (OSE-18840, September 2007)
- FY 2007 FISMA Assessment of Patent Search System—Primary Search and Retrieval (OSE-18841-1, September 2007)
- FY 2007 FISMA Assessment of Project Performance Corporation General Support System (OSE-18841-2, September 2007)
- Progress Being Made in Certification and Accreditation Process, But Authorizing Officials Still Lack Adequate Decision-making Information (OSE-19019, September 2006)
- SARSAT's E-Authentication Controls Do Not Provide Adequate Assurance of Users' Identities (OSE-1820, September 2006)

In-Progress Review

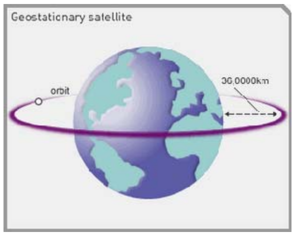
- FY 2009 FISMA Assessment of the Bureau of Industry and Security's IT Infrastructure System

3. Effectively Manage the Development and Acquisition of NOAA's Two Environmental Satellites

NOAA is modernizing its environmental monitoring capabilities, spending billions of dollars on two satellite systems that provide critical data: the National Polar-Orbiting Operational Environmental Satellite System (NPOESS) and Geostationary Operational Environmental Satellite-R Series (GOES-R). Space acquisitions like NPOESS and GOES-R are highly technical and complex and have a history of cost overruns, schedule delays, and performance failures. The costs and schedules of both of these systems have significantly increased since the projects commenced. They therefore require careful oversight to minimize any further disruption and to prevent any gaps in satellite coverage—a situation that could have serious consequences for the safety and security of the nation.



The $12.5 billion NPOESS project will provide continuous weather and environmental data for longer term weather forecasting and climate monitoring through the coming 2 decades.[1] The initial project plan called for the purchase of six satellites at a cost of $6.5 billion, with a first launch in 2008. But problems with a key sensor—the Visible/Infrared Imager Radiometer Suite (VIIRS)—were a major contributor to the increase in estimated cost, even as the number of satellites was reduced to four and the first launch pushed back to 2013. Recent analysis indicates that the $12.5 billion estimate could substantially increase in the near future.



The $7.7 billion GOES-R[2] system will offer an uninterrupted flow of high-quality data for short-range weather forecasting and warning, and climate research through 2028. An inadequate acquisition and management process contributed to underestimated costs for GOES-R and planned satellite capabilities that were too ambitious. As a result, the projected cost of GOES-R has increased from $6.2 billion to $7.7 billion, a major sensor has been removed, and the number of satellites to be purchased has decreased from four to two.[3]

[1] The cost of the NPOESS program is shared equally by NOAA and the Department of Defense.

[2] The GOES series of satellites have, since 1975, provided the United States with critical meteorological data for weather observation, research, and forecasting. Satellites in production are given letter designations, which are changed to numbers after reaching orbit.

[3] An option for two additional satellites is included in the contract.

Reining in additional costs and delays in both programs requires very specific action and vigilant oversight. For NPOESS, the three agencies developing the system—NOAA, NASA, and the Department of Defense—must (1) control and resolve the continuing problems with VIIRS, and (2) improve triagency decision making.

For GOES-R, NOAA needs to (1) work closely with the Department to ensure it follows best practices in overseeing the acquisition while awaiting development of formal Commerce oversight polices and procedures, and (2) work with Congress to update the baseline life-cycle cost estimate used in its annual reporting on the satellite system.

Continuing VIIRS problems jeopardize NPOESS mission

Despite scaling back the program in 2007, NOAA reports continuing problems with VIIRS development, among them that the subcontractor has sacrificed quality to meet the schedule, failed to follow rigorous development and test procedures, and still does not have a permanent project team. The primary contractor for NPOESS has been unable to correct these problems. So an integrated program office team will work on-site with the subcontractor to help finish VIIRS development. An independent review team is investigating alternatives in the event VIIRS cannot be built successfully. If these problems are not resolved with some expediency, it could mean further delay for the launch of a pilot mission to test the new VIIRS instrument and may result in gaps in data coverage. Because NPOESS is the only source of critical weather and environmental data, it is especially important that VIIRS problems be resolved and congressional confidence in and support of the program maintained.

Oversight structure has not been an effective mechanism for decision making

As joint project sponsors, NOAA, NASA, and Defense have direct oversight for the program through a triagency committee comprised of senior officials from each agency, but the committee has limited decision-making authority. For example, key acquisition documents initiated in June 2006 to formalize fundamental aspects of NPOESS management, testing, and cost, schedule, and performance baselines have not yet been finalized because their acceptance must be coordinated at higher agency levels.[4] NOAA is forming an independent review team to assess, among other things, the effectiveness of

[4] The four key documents not yet signed are the NPOESS Tri-Agency Memorandum of Agreement, Acquisition Program Baseline, Acquisition Strategy Report, and Test and Evaluation Master Plan.

the triagency management structure. The team plans to report preliminary findings in January 2009. The challenge for NOAA is to gain consensus among its partners on how to make the committee a responsive decision-making body.

NOAA and the Department need to follow accepted oversight procedures for the GOES-R acquisition

GOES-R is wholly funded by Commerce, though the satellites will be developed and acquired jointly with NASA. The structure of the program has introduced a new element of risk: NOAA now has the lead management role over the entire program (ground and space segments)[5] for the first time, giving the Department direct oversight responsibility as well. Our evaluation in 2007 found that significant weaknesses in oversight during earlier phases of the program led to the cost increases and schedule delays. Because GOES-R was not using an accepted life-cycle process, oversight officials were left without sufficient decision-making information. To address this problem we recommended, among other things, that the Department overhaul its major systems acquisition policy and NOAA identify how NASA management and oversight procedures would be followed for the entire program. NOAA and the Department took several significant actions in response to our review. NOAA finalized a GOES-R management control plan, which describes how NASA procedures will be applied, the Secretary delegated authority for key decisions to NOAA, and the Department has been working on a new major systems acquisition policy. However, the policy may not be ready before award of the GOES–R space and ground segment contracts in December 2008 and May 2009. In the absence of a revised policy, NOAA needs to work with the Department to develop effective interim oversight procedures prior to the planned awards.

NOAA needs to work with congressional committees on GOES-R reporting

The Mikulski Amendment to the 2008 Consolidated Appropriations Act requires NOAA to notify Congress[6] should GOES-R costs increase by 20 percent or more over the established baseline. However, the baseline used in the amendment is the cost estimate reported in NOAA's FY 2008 presidential budget request ($6.9 billion). At that point, too little was known about the GOES-R program to develop a reliable estimate. Since that time,

[5] In prior NOAA-NASA satellite programs, NASA managed the space segment.

[6] Notification is to be made to the Senate Committee on Appropriations and Committee on Commerce, Science, and Transportation; and the House Committee on Appropriations and Committee on Science and Technology.

the acquisition approach has been changed, the performance capabilities have been redefined, and the design has been refined, which resulted in the current $7.7 billion estimate. This projection is a more realistic and reliable baseline: it was developed in close collaboration with NASA, with guidance from a highly qualified independent review team, and with the benefit of an independent cost estimate. Although the current estimate does not breach the act's 20 percent cost growth threshold, NOAA should work with Congress to reestablish the baseline at the new, more realistic level.

For more information, view the documents below at www.oig.doc.gov:

Reports:

- Successful Oversight of GOES-R Requires Adherence to Accepted Satellite Acquisition Practices (OSE-18291, November 2007)
- Poor Management Oversight and Ineffective Incentives Leave NPOESS Program Well Over Budget and Behind Schedule (OIG-17794, May 2006)

4. Establish a Safety Culture at NIST

A June 2008 plutonium spill at the National Institute of Standards and Technology's Boulder, Colorado, laboratory raised serious concerns about NIST's ability to perform state-of-the-art research with radioactive and other dangerous materials while protecting the safety of workers and the community at large.

The plutonium spill was one of several incidents reported at NIST labs in the past few years that have revealed management flaws and a lax safety culture at the agency. But it was by far the most serious in terms of the potential for widespread harm.

Trace amounts of the material were subsequently found in the urine of several lab employees, but fortunately at levels too low to be dangerous. Moreover, small amounts of the material were discharged inappropriately into a laboratory sink and into restroom sinks. There is no evidence yet that any of the material reached the Boulder sewer system, but NIST has had to close the lab for decontamination—a process that NIST estimates will cost approximately $2.5 million with a scheduled completion date of April 2009. The time and cost required to fix the spill's underlying causes will likely be much greater.

Spill exposed weaknesses in NIST's safety management that must be corrected

The plutonium spill prompted a series of reviews by independent health and safety experts, the Department of Energy, and NIST's Ionizing Radiation Safety Committee, all of which shared a common finding—a commitment to safety at NIST Boulder is seriously lacking.

The Department of Energy found, among other things, that NIST had not established a safety management system or protocols. Safety roles and responsibilities were poorly defined, and the labs did not have the staff expertise to understand and analyze exposures to hazardous materials.

An independent reviewer noted that Boulder management does not consider safety to be its responsibility, but rather that of internal health and safety staff. And this staff had been told that safety must not interfere with creativity. One manager conveyed his misplaced sense of responsibility during an annual safety walk-through by talking on his cell phone rather than paying attention to conditions in the lab.

In addition, the circumstances under which the spill occurred are evidence that safety is not a core value: a guest researcher was allowed to work alone with the plutonium after normal business hours even though he had no training in handling radioactive materials.

NIST's management structure has not supported a safety culture

In its FY 2006 annual report on NIST's strategic direction, performance, and policies, the Visiting Committee on Advanced Technology[7] noted inconsistencies in safety procedures across NIST laboratories, and stated that "Safety is a leadership activity that senior NIST leadership must be actively involved in." In principle, NIST management is committed to safety. But as a practical matter safety has not been a clearly delineated function within its organizational structure, and this contributed to the numerous lapses that occurred leading up to the spill.

The director's position at Boulder had no line management authority for staff at the campus. In effect, then, at the time of the spill, no one on-site had overall management responsibility for the safety of the work being conducted in Boulder or for managing the response to the incident. The then-director of the Boulder campus put it simply: "No one was in charge."

NIST Boulder had only recently received permission to work with plutonium. There was no systematic, integrated management process for analyzing and preparing for the risks associated with this new work, for strictly managing the material once it arrived, for dedicating lab space to radioactive materials research, for ensuring personnel were properly trained to work with the plutonium, or for responding to related emergencies. Though NIST has issued a number of safety protocols over the years, such as the *Laboratory Safety Manual* and *Safety Operation System*, managers and staff at Boulder were not involved in developing them, were generally unfamiliar with their requirements, and often viewed them as voluntary guidelines. The lab was even found to be potentially noncompliant with several required federal and industry safety standards.

An analysis of Boulder safety staffing conducted by the on-site safety office found that NIST would need 13 full-time workers to properly perform safety functions it currently handles with only 5. At present, NIST addresses this staffing deficiency by simply deferring many safety tasks and by requiring

[7] The Visiting Committee on Advanced Technology was established by the Omnibus Trade and Competitiveness Act of 1988. The committee reviews and makes recommendations regarding general policy for NIST, its organization, its budget, and its programs to the Secretary of Commerce and Congress.

staff to work significant amounts of overtime—which could cause employee fatigue and indirectly result in more accidents.

NIST facilities must comply with safety requirements

The plutonium spill and the subsequent revelations regarding NIST's lax safety culture are particularly disturbing in light of the agency's international reputation as a world-class scientific organization. Yet rather than modeling best practices, NIST's lax approach to safety increases risks to the agency and the greater community.

Two studies conducted by NIST have identified a backlog of more than $500 million in facility maintenance and repair requirements. A 2004 study found $458 million in deficiencies at NIST's Gaithersburg campus and a 2008 study identified $48 million in deficiencies at Boulder. Many of the items relate directly to safety. NIST noted that it should be investing at least $50 million to $70 million annually to bring its facilities to a "fair" condition and stay ahead of further deterioration. According to the Department, NIST received $32 million for facilities in FY 2008.

It is clear from the circumstances surrounding the plutonium incident and subsequent revelations that, at a minimum, NIST must make safety a primary concern at all organizational levels and strictly comply with all federal requirements and industry standards. It must establish and enforce stringent policies and procedures for handling hazardous materials and strict lines of accountability for implementing them.

At the request of the Deputy Secretary, the Office of Inspector General is reviewing safety at NIST, with a specific focus on the agency's management structure as it relates to safety, as well as its policies and procedures for handling radioactive materials. We are examining NIST's systems for identifying safety resource requirements, allocating resources to safety, and addressing safety requirements in planning and budgeting for its work.

For more information, view the documents below at www.oig.doc.gov:

In-Progress Reviews

- OIG Review of NIST Management Structure and Safety and Training Systems in Response to Deputy Secretary Request
- Joint OIG/Nuclear Regulatory Commission Investigation of NIST's Compliance with its Special Nuclear Materials License

5. Ensure NTIA Effectively Carries Out Its Responsibilities Under the Digital Television Transition and Public Safety Act

The Digital Television Transition and Public Safety Act of 2005 assigned the National Telecommunications and Information Administration responsibility for implementing a $2.5 billion initiative for the conversion to digital television and improvements to public safety communications. The act authorizes NTIA to use $1.5 billion to support the nation's February 2009 switch to all-digital broadcasting by offering coupons toward the purchase price of converter boxes that will enable analog television viewers to receive digital programming.

A primary purpose of the switch to digital television is to free up radio frequencies for advanced wireless emergency communications at state and local levels, thus improving the ability of first responders to communicate with one another during emergencies. The act authorizes NTIA to provide approximately $1 billion in grants for public safety interoperable communications (PSIC) projects in all 50 states, the District of Columbia, and the U.S. territories—a total of 56 entities. This is a significant undertaking for NTIA, whose prior experience administering grants has been with two small programs: the Public Telecommunications Facilities Program, whose FY 2008 funding availability was just $16.8 million, and the discontinued Technology Opportunities Program, which issued a total of $233 million in grants during its 10-year span (1994-2004).

The authorizing legislation requires NTIA to coordinate with the Department of Homeland Security in administering the PSIC program and set a statutory deadline of September 30, 2010, to expend grant funds. Subsequent legislation set a statutory deadline of September 30, 2007, for the award of grants.

Converter Box Coupon Program is progressing with few problems, but close oversight must be maintained

NTIA has made substantial progress in helping prepare television viewers for the switch to digital broadcasting: in August 2007 it contracted with IBM to provide certain services to implement the $1.5 billion Converter Box Coupon Program. The program offers up to two $40 coupons per household to offset the purchase price of the boxes, which will enable consumers who rely on analog signals for television reception to receive digital broadcasts after February 17, 2009. NTIA had issued more than 26 million coupons as of September 30, 2008, and redeemed 10 million of them. Although television stations will cease analog broadcasting on February 17, consumers can request coupons until March 31, 2009, or while supplies last.

Maintaining strict accountability for funds in a program of this type and size requires careful oversight and strong internal controls to guard against fraud, waste, and abuse among retailers and to ensure the program is properly closed out by September 2009, as required by the act. Potential fraud schemes include selling the free coupons to consumers, or retailer redemption of coupons for converter boxes that were not provided. NTIA has not yet discovered any egregious instances of waste, fraud, and abuse, but has decertified 16 retailers for violating program rules.

As the program moves toward completion, NTIA should continue to update and strengthen its internal controls to reflect evolving program requirements and circumstances, such as recent program rule changes that make coupons available to residents of nursing homes, intermediate care facilities, assisted living facilities, and households that use a post office box for residential mail delivery. Based on its own analysis, NTIA believes it is prepared to handle a significant uptick in coupon demand as the transition date approaches.

Although administering the coupon program is NTIA's primary role, the act authorizes the agency to use up to $5 million for outreach and education to ensure that consumers know about both the digital TV transition and the coupons. NTIA has targeted geographic areas and demographic groups that have the highest percentage of analog-only households. The outreach strategy provides for intensified publicity at critical points in the conversion, such as the approach of the February 17, 2009, switch and the March 31 deadline for coupon requests. However, there are bound to be households that do not get the message in time and find themselves without television reception on February 17. Although the Federal Communications Commission (FCC) has primary responsibility for consumer education and outreach, NTIA should continue to work with stakeholders, including representatives of at-risk groups, to ensure a smooth transition to digital television.

Grantees may not be able to complete projects within the legislation's short funding time frame

The PSIC program is a one-time grant opportunity to target specific funds and resources toward improving the interoperability of local and state voice and data communications. But grantees are moving slowly, and whether they can complete their projects by the statutory deadline of September 30, 2010, is questionable.

As of September 2008, grantees had spent less than 1.5 percent of the available $1 billion, which leaves them only 2 years to complete their projects or lose funding. But many of the projects involve activities that could take much longer: GAO found that acquiring and deploying interoperable communications equipment and infrastructure in similar Homeland Security grants programs was slowed by state-imposed legal and procurement requirements.[8] These could also impact the PSIC program, as well as other considerations: for example, PSIC grantees may need to obtain FCC licenses —a process that can take months—before they can erect communications towers to support interoperability. Time must also be factored in for training responders to use the systems once they are up and running. Under PSIC's authorizing statutes, money not spent within the 3-year term will be returned to the Treasury.

In September and October 2008 we contacted 22 grantees, including 19 of the 20 receiving the largest grants. Only one of the 22 grantees stated that it plans to acquire most of its interoperable communications equipment within the next 6 months. Eight of the 22 stated that they are in the early stages of planning their acquisitions. The other 13 will start acquiring most of their interoperable communications equipment in late FY 2009 or possibly in the beginning of FY 2010. Given all that must follow the purchase of equipment—installation, operational testing, and training, at a minimum—grantees who are still in the acquisition stage as late as FY 2010 face the very real possibility of arriving at the program's September 30 deadline with partially completed projects but without funding to finish them out.

NTIA must consider options for ensuring the program achieves its objectives

Part of the reason for the grantees' slow start is the way the PSIC awards process worked. Because of the September 30, 2007, award deadline imposed by the Call Home Act of 2006, PSIC awards preceded approval of individual project plans and release of funds. This was unlike other Commerce grants programs, which award grants competitively, based on the merit of a project's proposal. As a result, many recipients spent the first year of the 3-year grant period developing plans, obtaining their approval, and awaiting availability of funds.

[8] U.S. Government Accountability Office, March 11, 2008. *Homeland Security: DHS Improved its Risk-Based Grant Programs' Allocation and Management Methods, But Measuring Programs' Impact on National Capabilities Remains a Challenge*, GAO-08-488T. Washington, D.C.

NTIA should expeditiously identify grantees that are at high risk of not meeting the statutory deadline for completing their projects, give them the technical assistance they need to accelerate the process, carefully monitor their progress, and keep Congress informed of the PSIC program's status toward achieving its objectives. If any entities seem still unlikely to meet the deadline, NTIA should work with Congress to extend it.

For more information, view the documents below at www.oig.doc.gov:

In-Progress Reviews

- NTIA Should Further Improve Digital-to-Analog Converter Box Coupon Program Internal Controls to Prevent Fraud, Waste, and Abuse (CAR-19004-1, draft October 2008, final estimated November 2008)
- First Annual Assessment of Public Safety Interoperable Communications Grants (DEN-19003, draft estimated November 2008, final estimated January 2009)
- Audits of Public Safety Interoperable Communications Grants for Arkansas, Louisiana, Pennsylvania, and Nevada.

Other Issues Requiring Significant Management Attention

Several other Commerce operations and activities present distinct challenges, and their resolution is essential to the Department's sound management and mission success. The first—acquisition management—has ramifications Department-wide. The remaining three—though agency-specific—have a direct bearing on U.S. economic strength and competitiveness, environmental protection, or national security.

Weaknesses in the Department's Acquisition Oversight and Acquisition Workforce

Acquisition and contract management has been a consistent watch list item for inspectors general and GAO, as related government spending has ballooned in recent years. Spending on contracts government-wide, for example, has more than doubled since 2000—from $208 billion to $430 billion in FY 2007—while the federal acquisition workforce has remained fairly constant: roughly the same number of skilled professionals now oversee more than twice as many federal contract dollars as they did 7 years ago, and the projects they support have greatly increased in complexity and risk.

Shortfalls and failures in major systems acquisitions are all too common in federal programs. And contracts of all sizes and complexity are at risk for fraud and waste because of poor oversight and lax controls.

Over the next 2 years, the Department of Commerce will spend an average of approximately $3 billion annually on goods and services. The 2010 decennial census and two critical NOAA satellite systems will account for roughly a third of these annual expenditures. All three of these programs have already suffered significant cost overruns and schedule delays because of poor acquisition management.

The Department does not have coherent policies to guide systems acquisition or effective oversight mechanisms, and these failings were major contributors to the problems we identified with NOAA's GOES-R satellite program and the Census Bureau's Field Data Collection Automation contract. It also lacks a sufficient amount of skilled contracting and project management expertise—a problem all federal agencies are grappling with. Hiring and retaining a skilled acquisition workforce has been difficult, and the competition stiff. Commerce has a limited number of contracting specialists to meet its multibillion-dollar workload. It has no reliable count of its program and project managers or contracting officer's technical representatives, although skilled professionals in these positions are also at a premium.

The Department is working to address these problems, but the process is slow and in its early stages. Commerce is strengthening acquisition and contracting by updating its antiquated policies and procedures to promote more effective planning, implementation, and oversight. It is also taking steps to make better use of its oversight bodies—the Acquisition Review Board and the Commerce Information Technology Review Board—and to integrate their activities, to ensure acquisition plans are appropriate, and programs and contracts are reviewed at key decision points in their life cycle.

But success in these efforts will not be enough to improve the Department's overall acquisition operations without commensurate success in hiring and retaining a qualified acquisition workforce. The pool of applicants for these jobs is not large, and the looming retirement of some 50 percent of the current federal acquisition workforce over the next 10 years may well push shortages beyond the critical point.

OMB, the Federal Acquisition Institute, and the Office of Personnel Management recently launched the Federal Acquisition Intern Coalition to attract interest in federal contracting among college students. The Department needs a comprehensive human capital strategy that (1) taps into such recruiting initiatives, (2) explicitly defines what acquisition skills and competencies it needs and how they will evolve over the short- and long-term, and (3) offers professional development and other incentives to attract and keep qualified candidates.

For more information, view the documents below at www.oig.doc.gov:

Reports
- The Office of Acquisition Management Has Not Implemented New Contracting Policies in a Timely Manner (IPE-19045, June 2008)
- The National Data Buoy Center Should Improve Data Availability and Contracting Practices (IPE-18585, May 2008)
- Successful Oversight of GOES-R Requires Adherence to Accepted Satellite Acquisition Practices (OSE-18291, November 2007)

In-Progress Reviews
- Audit of the Field Data Collection Automation Contract Type and Award Fee

USPTO's Long and Growing Patent Processing Times, and Its Financing Vulnerabilities

The efficiency with which the U.S. Patent and Trademark Office processes patent applications has a direct bearing on how well it achieves its mission of promoting U.S. competitiveness. Meeting the demand for new patents in a timely manner has been a long-standing challenge for USPTO. Increases in both the volume and complexity of patent applications have lengthened application processing times and backlogs dramatically. In 2004, USPTO had a patent backlog of nearly a half-million applications and average processing times of 27 months. By 2007, processing times averaged nearly 32 months, with wait times for communications-related patents as long as 43 months. As of September 30, 2008, USPTO reported a backlog of 750,596 applications and estimated that the backlog will exceed 860,000 by September 2011. USPTO needs to reverse the upward trend and continue to implement measures discussed in its 2007-2012 strategic plan that have a significant impact on reducing the backlog, such as shortening application review times, improving examiner error rates, and hiring, training, and retaining skilled examiners.

USPTO's unique financing structure also presents challenges. There is a complex relationship between the number of patent applications filed, the size of the application backlog, the number of patents issued, and the fees USPTO collects in connection with the patent process. The agency uses fees collected today to pay for patent applications filed and examined in prior years. With the backlog growing, processing times increasing, and the number of patents issued flattening, this method of financing could become increasingly risky. The current model for financing USPTO's critical mission warrants attention to ensure that it will continue to provide sufficient funding to process all backlogged applications as well as any newly filed.

For more information, view the document below at www.oig.doc.gov:

In-Progress Reviews

- Audit of USPTO's Quality Assurance Process

NOAA's Ability to Conserve the Nation's Fragile Oceans and Living Marine Resources While Ensuring a Vital U.S. Commercial Fishing Industry

According to NOAA, 3.5 million square miles of our coastal and deep ocean waters and the Great Lakes support over 28 million jobs—one of every six—in the United States, and the value of the U.S. ocean economy tops $115 billion. But these economic benefits come at great cost as the health of our oceans and coastal ecosystems continues to decline in the face of increasing coastal development, pollution, overfishing, and the destructive impact of invasive species.

Charged with maintaining and improving the viability of marine and coastal ecosystems while supporting global marine commerce and transportation, NOAA manages a significant portion of the federal government's investment in living marine resources. It faces difficult challenges in promoting the health of these resources while ensuring they sustain the vital economic benefits we derive from them.

In January 2007, the President signed the reauthorized Magnuson-Stevens Fishery Conservation and Management Act, which requires annual catch limits, an end to overfishing by 2011, and better integration of fishery management planning with national environmental review procedures to ensure the environmental impacts of any significant ocean activity under consideration are thoroughly vetted. The challenge for NOAA will be to implement these new requirements in a manner that improves the status of our marine resources without undermining the health of the U.S. fishing industry. To fulfill its mandates for living marine resources, NOAA also needs to take action to rebuild populations of protected species, conserve important habitats, and undertake the science programs necessary to improve its understanding of complex marine ecosystems.

For more information, view the documents below at www.oig.doc.gov:

Reports

- National Marine Sanctuary Program Protects Certain Resources, But Further Actions Could Increase Protection (IPE-18591, February 2008)
- NOAA's Management of the Joint Enforcement Agreement Program Needs to Be Strengthened (IPE-19050-1, September 2008)

In-Progress Reviews

- Audit of NOAA's Direct Loan Program
- Review of Allegations that NMFS' Northeast Region Is Not Using the Best Available Science in Management Decisions

BIS' Setbacks in Modernizing Its Obsolete Information Technology Infrastructure to Strengthen the Dual-Use Export Control System

In January 2007, GAO added the Bureau of Industry and Security's dual-use export control system to its government-wide high-risk list. One of the key challenges facing BIS in ensuring that the dual-use export control system is properly equipped to advance U.S. national security, foreign policy, and economic interests is the replacement of its obsolete Export Control Automated Support System (ECASS). BIS' core export administration and enforcement business processes are directly supported by ECASS. Approximately 450 federal staff and 28,000 exporters currently use the system. However, the database structure—originally deployed in 1984—is complex and no longer supported by the technology industry. The effort to modernize ECASS began in 1996, but the project has been underfunded and beset by technical problems and schedule slips that current management has been attempting to address in a budget-constrained environment.

The current projected completion date for the ECASS modernization is FY 2014. Based on our interviews, the total funding requirements for ECASS modernization are not clearly established. BIS must provide a comprehensive plan for what is required to modernize ECASS, including how much it will cost and how it will avoid the management and technical problems experienced in past modernization attempts.

Enhancing the performance of ECASS and ensuring continued operation of an effective licensing information system are far too important to postpone any longer. BIS must demonstrate that it has a modernization strategy and plan in place to convincingly make the case for increased funding, or develop a plan to implement its ECASS modernization effort with existing resources (i.e., reallocate existing funding).

For more information, view the documents below at www.oig.doc.gov:

Reports

- Annual Follow-Up Report on Previous Export Control Recommendations, as Mandated by the National Defense Authorization Act for Fiscal Year 2000, as Amended (IPE-18546, March 2007)
- BIS Needs to Strengthen Its ECASS Modernization Efforts to Ensure Long-Term Success of the Project (IPE-14270, February 2002)

Acronyms and Abbreviations

BIS	Bureau of Industry and Security
BEA	Bureau of Economic Analysis
C&A	Certification and Accreditation
CSAM	Cyber Security Assessment and Management
ECASS	Export Control Automated Support System
GAO	Government Accountability Office
GOES-R	Geostationary Operational Environmental Satellite-R Series
FCC	Federal Communications Commission
FDCA	Field Data Collection Automation
FISMA	Federal Information Security Management Act
NESDIS	National Environmental Satellite, Data, and Information Service
NIST	National Institute of Standards and Technology
NOAA	National Oceanic and Atmospheric Administration
NMFS	National Marine Fisheries Service
NPOESS	National Polar-Orbiting Operational Environmental Satellite System
NTIA	National Telecommunications and Information Administration
NWS	National Weather Service
OMB	Office of Management and Budget
PSIC	Public Safety Interoperable Communications
SARSAT	Search and Rescue Satellite-aided Tracking
USPTO	United States Patent and Trademark Office
VIIRS	Visible/Infrared Imager Radiometer Suite