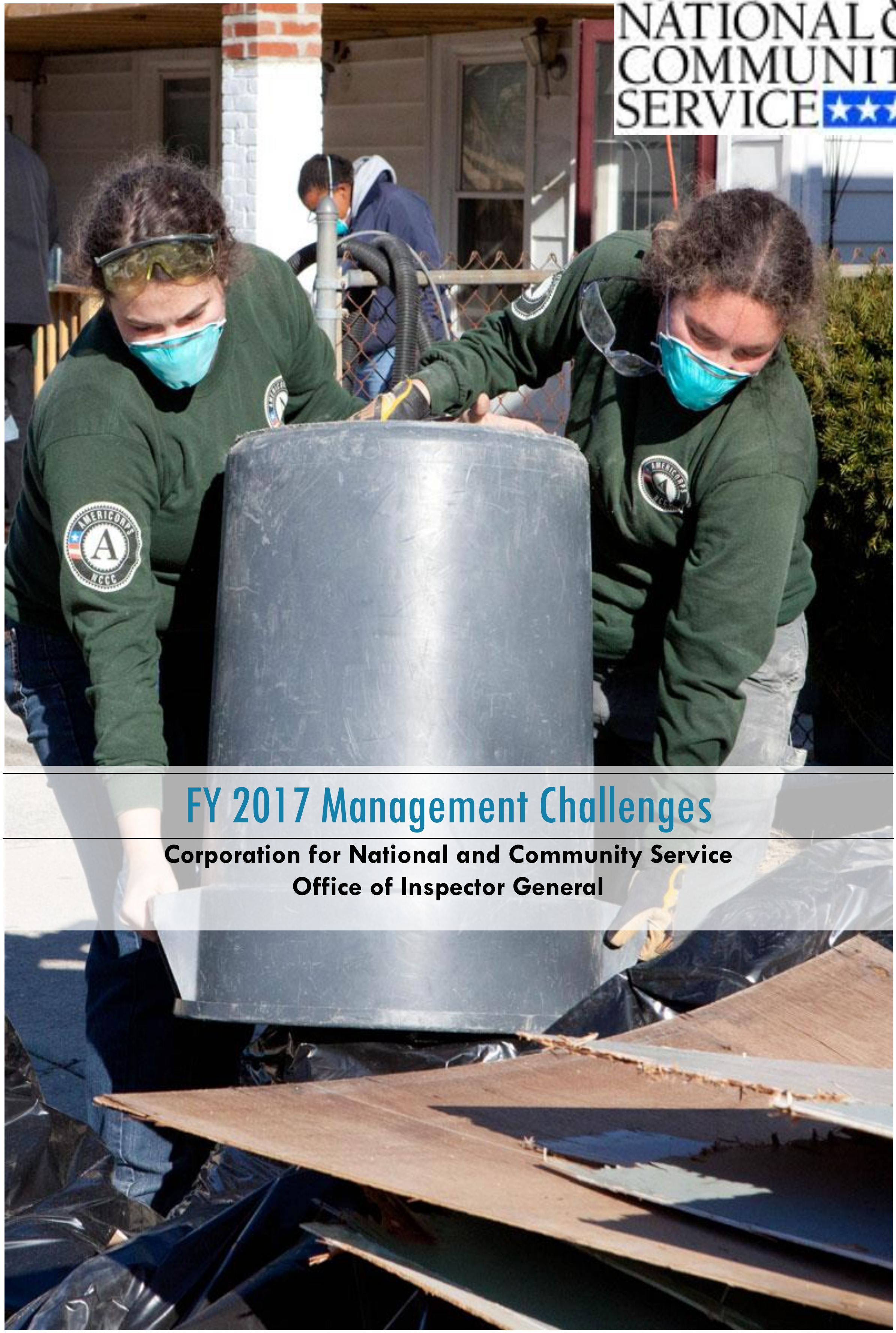
Office of Inspector General

Corporation for NATIONAL & COMMUNITY SERVICE



# FY 2017 Management Challenges

**Corporation for National and Community Service**
**Office of Inspector General**

Office of Inspector General
Corporation for
NATIONAL &
COMMUNITY
SERVICE

December 7, 2016

TO: Wendy Spencer
Chief Executive Officer

FROM: Deborah J. Jeffrey
Inspector General

SUBJECT: Management Challenges for Fiscal Year 2017

This report identifies management and performance challenges facing the Corporation for National and Community Service (CNCS or the Corporation). We selected these challenges by considering past and ongoing audit, review and investigative work, as well as discussions with CNCS management regarding existing vulnerabilities. We also considered new activities that could pose challenges because of their breadth and complexity.

The FY 2017 management challenges are:

1. Strengthening Grant Oversight and Monitoring
2. Protecting the Communities We Serve with Thorough Criminal History Checks and Prevention Measures
3. Reducing Improper Payments
4. Securing Information Systems and Modernizing Information Technology
5. Rethinking the Fundamentals to Support National Service

We look forward to working with CNCS to address these challenges in the coming year. If you have any questions or would like to discuss these issues, please contact me at (202) 606-9366.

## TABLE OF CONTENTS

## Management Challenge 1: Strengthening grant oversight and monitoring

CNCS continues to struggle to provide effective oversight of its grant portfolio, leaving these funds unnecessarily vulnerable to waste, fraud, mismanagement and abuse. Effective monitoring is impeded by a series of legacy burdens, including frequent turnover in staff and key leadership positions; the historic lack of experience, sophistication and resources in the office responsible for developing grant monitoring strategies and protocols; and outdated information technology that does not support data analytics and other modern oversight tools.

Disciplined grant oversight at CNCS is necessary, because grant-making is the agency's core activity. At any given time, CNCS must oversee more than 2,100 active grants, ranging in size from $40,000 to ten million dollars, in the seven programs that it operates throughout the United States and its Tribes and Territories. These grants account for three-quarters of the Corporation's $1 billion appropriation. Grantees include well-established national nonprofits, such as the Red Cross, major research universities, State and local governments, and small community-based organizations for which CNCS provides the majority of funding. Not surprisingly, these grantees vary greatly in resources, capabilities, experience and infrastructure.

Both internally and in external reporting, CNCS-OIG has repeatedly identified weaknesses in the Corporation's monitoring of its grantees, as designed and as implemented. Investigations and audits of grantees regularly uncover serious problems that were overlooked in routine monitoring. CNCS has not updated its approach to grant monitoring for many years.

Key Congressional stakeholders (including supporters of CNCS and its programs) have expressed concerns about the rigor of the Corporation's grant oversight. Twice in the last five years, the House Committee on Education and the Workforce, Subcommittee on Higher Education and Workforce Training, has held hearings critical of accountability at CNCS.[1] The Government Accountability Office (GAO) is in the final stages of a study of CNCS's grant monitoring, undertaken at the bipartisan request of the House Committee on Oversight and Government Reform. We expect that evaluation to identify fundamental changes essential to strengthen grant monitoring.

[1] The most recent hearing, conducted on May 24, 2016, can be found at http://edworkforce.house.gov/calendar/eventsingle.aspx?EventID=400691

The Corporation needs to replace its existing grant oversight philosophy and practices with a rigorous, tested, risk-based approach to grant monitoring. Thoughtful application of risk management principles offers a significant opportunity to improve stewardship at CNCS. In April 2016, CNCS filled the newly created position of Chief Risk Officer with an experienced risk-management professional. This new expertise at the executive level provides CNCS with the capability and leadership to make necessary changes.

## Limitations of existing grant monitoring

Currently, the Corporation decides annually which grantees it will monitor closely by assessing each grant according to a uniform set of 19 criteria, which it treats as risk indicators. It applies the same 19 criteria across the entire grant portfolio, notwithstanding critical differences among CNCS programs and grant vehicles that bear directly on risk. The model also omits significant risks identified in CNCS-OIG audits and investigations. CNCS uses this model to calculate a single risk score for each grant and generally applies the same set of monitoring procedures to all grants rated as high risk. Despite relying heavily on this model, CNCS has never validated it against outcomes.

The entire grant monitoring program rests on assumptions that are untested. CNCS-OIG audits and investigations often uncover major problems at grantees that the Corporation has rated as low or medium risk and therefore not scrutinized closely. A preliminary analysis undertaken by CNCS-OIG several years ago showed that the 19 criteria do a poor job of predicting which grantees will produce catastrophic outcomes, such as going bankrupt while owing large sums to the Corporation, closing their doors in the midst of a grant or requiring CNCS to terminate a grant for cause.

CNCS conducts virtually all of its grant monitoring manually, like its other internal controls. Manual processes are subject to human error and are easily disrupted due to overwork, inattention or conflicting priorities. Program officers perform the majority of the monitoring, and many of them do not have the training or the skills to identify and correct deficiencies in grantee's financial management systems and practices. Having the risks assessed by the same program officers and grant officers who assist a grantee also introduces a strong potential for bias. The closest monitoring takes the form of a site visit to a grantee, which may occur only once every six years. Program officers visit no more than a fraction of subgrantees or operating sites.

Beyond the accuracy of its risk assessments, CNCS has never evaluated the effectiveness of grant monitoring or how the agency could perform better. Rather, the Corporation tests its internal controls over grant monitoring solely by reviewing paper compliance, e.g., whether reports are submitted on time and whether the proper approvals are on file.

Despite these limitations, CNCS leadership has for many years touted its grant monitoring as highly sophisticated and risk-based. This exaggerated portrayal is not based on any data. This practice has encouraged complacency inside the agency, stifled any urgency about improvement of the Corporation's core function and increased resistance to change.

## Moving towards risk-based grant monitoring

The new government-wide requirement that agencies transition to Enterprise Risk Management and the selection of an experienced Chief Risk Officer offer an opportunity for CNCS to develop a more sophisticated, risk-based approach to grant oversight, to be regularly evaluated and continuously improved. A more disciplined approach to risk will help CNCS direct its limited oversight resources where they will have the greatest impact. Establishing risk-based grant monitoring will require CNCS to return to the fundamentals: (1) identifying the risks associated with its grants, including fraud risks; (2) categorizing and ranking them; (3) developing indicators that align to those risks, taking into consideration differences among grantees, stages of the grant lifecycle, programs and activities; and (4) developing oversight activities suited to particular risks. The forthcoming GAO study should be of some assistance in this task; CNCS should also make better systematic use of CNCS-OIG audits and investigations.

This new risk model should inform every aspect of grant management, including:

- Grant competition, *e.g.*, determining what information CNCS should solicit in its grant application and obtain from third-parties, as well as how that data is to be assessed in the award process;

- Considering in grant award decisions a realistic assessment of CNCS' capacity to manage risks, the optimal mix (within each program and across the portfolio) of low-, medium- and high-risk grants. Creating a plan for managing the risks associated with each grant and imposing appropriate special conditions;

- Expanding the menu of monitoring activities and customizing/targeting them to specific risks, to avoid wasting resources monitoring *de minimis* risks;

- Smart design of testing for improper payments (*see* Management Challenge 3) to complement and cross-check aspects of grant monitoring;

- Recruiting, training and retaining a qualified workforce, and assigning responsibilities based on the type of risks presented, including: (a) differentiating between programmatic and financial risks and assigning the latter to trained grant officers/financial staff for oversight; (b) rotating a portion of the portfolios of program and grant officers each year, to provide a fresh look, maintain objectivity and reduce the risk of over-identification with grantees; and (c) having certain risk assessments performed by trained staff other than those responsible for assisting the assessed grantees;

- Assessing risks by grantee, not simply by grant, and sharing information across program boundaries for grantees that receive funding from multiple programs;

- Updating key aspects of grantee risk assessments for consideration at continuation-of-funding decisions within the same three-year grant cycle;
- Adopting and enforcing a zero-tolerance approach to, and direct monitoring of, the most consequential risks and/or legal violations;

- Better use of technology and ready access to data analytics for routine monitoring, *e.g.*, for benchmarking and to identify anomalies, outliers and trends that warrant greater attention, and to reduce dependence on inefficient manual processes;

- A presumption that awards below a pre-determined dollar threshold will be fixed amount grants, thereby reducing the financial management burdens on grantees and allowing more effective use of CNCS monitoring resources; and

- Continuous improvement of the risk model and risk indicators to validate their accuracy, assess the incidence of particular problems and incorporate emerging risks.

## Cultivating a culture of accountability

All Corporation personnel, from the leadership on down, should be committed to holding themselves, one another and grantees accountable for the appropriate use of Federal resources and compliance with all applicable requirements. This means ending CNCS's historical reluctance to hold grantees to their commitments, absent intentional misconduct. Recovering improperly incurred costs from a nonprofit is not punitive; it is stewardship. Similarly, grantees should expect to consult with CNCS before altering the purpose and objectives of the grant. This means an end to condoning or retroactively approving violations of grant requirements, a practice that encourages grantees not to seek permission because they can confidently expect forgiveness.

In the last year or so, the Office of Grants Management has taken a more business-like approach to its work, favoring early intervention when a grantee cannot or will not live up to important obligations. Its leaders are more willing to disallow costs, promptly collect outstanding debts and press for timely resolution of audit findings. Rather than seeing this as punitive, they view it as good stewardship and strong oversight. However, they continue to encounter resistance from staff and grantees still entrenched in the prior permissive culture.

Though senior leaders have publicly endorsed accountability, they have sometimes acted in ways that fortified resistance to it.

Internally, senior leaders can strengthen accountability by inviting and willingly entertaining tough questions about the Corporation and its programs and not reflexively defending the status quo. CNCS personnel should be rewarded for questioning assumptions, identifying risks and suggesting changes.

In addition, CNCS needs a disciplined process for analyzing significant negative outcomes across all Corporation operations, to identify systemic gaps, red flags that were overlooked and human errors. The purpose of such an inquiry is not to assign blame but rather to understand what went wrong and to use the resulting insights to improve operations. Skipping this step, whether out of aversion to conflict or a desire not to dwell on failures, deprives CNCS of an opportunity to determine and address the root causes and may lead to ineffective responses.

## Management Challenge 2: Protecting the communities we serve by thorough criminal history checks and prevention measures

Ensuring the safety of the communities served by CNCS programs should be among the highest priorities of agency leaders. This requires that CNCS and its grantees prevent dangerous persons from exploiting grant-funded programs to gain access to at-risk individuals. Predators can do incalculable harm, and we know that many of them seek out opportunities to interact with vulnerable persons and may conceal their identities in order to do so. Vigilance in screening national service participants and staff is a moral, as well as a legal, imperative.

Mindful of these risks, Congress mandated in the Edward M. Kennedy Serve America Act of 2009 (the Serve America Act) that grantees exclude murderers and sex offenders from national service, prescribing specific sources that must be checked.[2] For members or grant-funded staff that work with vulnerable populations—children and youth, the elderly or persons with disabilities—the grantee must check the National Sex Offender Public Website (NSOPW), the criminal history repository of the state in which the individual resides and the state in which s/he will serve, and secure a fingerprint-based check from the Federal Bureau of Investigation

[2] An individual may not serve in a national service position if s/he was convicted of murder; is a registered or registrable sex offender; refuses to undergo a criminal history check; or makes a false statement in connection with a criminal history check.

(FBI). CNCS requires that the NSOPW check be *completed* before the member or staff begins service; the other checks must be *initiated* at that time, and the individual may not be alone with a member of a vulnerable population until the grantee receives results establishing that the individual has no disqualifying criminal history.

Many grantees have difficulty performing the required criminal history checks (CHCs). Grant audits conducted by CNCS-OIG have consistently found high rates of noncompliance, but, until recently, CNCS treated them as outliers and did not recognize the pervasiveness of failure to timely screen members and staff. Only when CNCS conducted a statistical analysis of grantee expenditures in FY 2014 was the agency forced to confront the substantial extent to which grantees fail to perform necessary checks when and as required. In FY 2016, despite mandatory training, self-assessment and an amnesty the prior year to encourage grantees to come into full compliance, the Office of the Chief Risk Officer found an stunningly high rate of failure to properly perform CHCs: 22 percent in AmeriCorps State and National, 36 percent in the Foster Grandparents Program (FGP), 40 percent in the Senior Companion Program (SCP) and 41 percent in RSVP. A recent internal survey of the three Senior Corps programs reported that one-quarter of Senior Corps grantees had some CHC noncompliance, and approximately 45 percent had policies that did not meet CHC requirements.[3] CNCS's FY 2016 statistical analysis of improper payments found that FGP spent $26.8 million, 34 percent of the program's total expenditures, to pay grant-funded staff and stipended members for whom the necessary checks were not completed or had not been documented. SCP spent $10.6 million, one-third of its costs, on members and staff with inadequate CHCs. In RSVP, the amounts were $9.5 million and 23 percent, respectively. The rates of noncompliance are alarming, as is the fact that CNCS failed to detect them in its routine monitoring of grantees.

Until recently, grantees faced little accountability for their noncompliance. When they discovered it, CNCS program officers responsible for oversight typically assisted grantees to complete the checks but often took no further action. As long as no currently serving members or staff were murderers or sex offenders, CNCS did not disallow costs for failures to perform CHCs. In 2011, CNCS adopted a written policy of disallowing all costs associated with service during the period of incomplete or untimely background checks, but did not enforce it with any regularity. This informal "no harm, no foul" policy rewarded grantees for being lucky, and excused recklessness with the safety of the communities they were supposed to serve. The enforcement environment did little to convey that grantees should regard background checks as a high-priority responsibility.

[3] Since Senior Corps allowed its grantees to select the files to be reviewed, the actual rate of noncompliance may be higher.

CNCS-OIG has consistently identified insufficient background checks as a critical risk for CNCS and its grantees. In FY 2015, CNCS adopted active measures to improve criminal background checking; they are an important first step. CNCS-OIG urges strengthening them as follows:

## Expanding Access to the Channeler

CNCS has recently contracted with a vendor, known as a channeler, to perform timely and compliant CHCs for grantees. As of October 2016, the channeler has conducted about one-quarter of the CHCs performed during the last nine months.

Outsourcing and consolidating CHC compliance avoids unnecessary duplication of effort by each grantee, allowing them to focus on programmatic activities, and ensures that experts perform this vital function. CNCS will likewise find it more efficient to monitor the performance of a single contractor, rather than attempting to oversee the efforts of thousands of grantees.

However, access to the channeler is limited to those grantees that cannot successfully conduct FBI fingerprint checks through their state criminal history repositories.[4] CNCS should maximize use of the channeler by eligible grantees and work actively to expand the current access. If necessary, the Corporation should seek legislative changes to facilitate this expansion.

## Focusing on safety and prevention vs. compliance

Many grantees assign low-level administrative staff to conduct their criminal background checks, treating this as a mere compliance exercise. CNCS must do more to distinguish CHC from garden-variety regulatory requirements. The CNCS CEO’s exhortation to conduct CHCs “on time, every time” has set an important tone from the top, and it must be reinforced so that it is more than a catchy chant.

Educating grantees about the risks of predators will help them understand CHC as a moral obligation. Background checking, though necessary, is not enough, because many offenders, particularly sex offenders, are never caught and convicted. It is therefore incumbent on CNCS to remind grantees that their responsibility to remain vigilant continues even after an individual passes a background check. Grantees, especially those that serve vulnerable groups, need the tools to prevent and identify potentially problematic conduct, policies and practices to minimize the risk of harm and strategies to intervene early. CNCS-OIG engaged the National

[4] This limitation was imposed at the insistence of certain states that derive revenue when CNCS grantees use the state repository as a conduit for their FBI checks.

Center for Missing and Exploited Children, which assists many nonprofits, to educate CNCS leaders about these subjects.

CNCS should increase the dissemination of prevention-related information in its grantee training. That training should remind grantees: (1) that the first obligation of service organizations is to protect, and avoid harming, the vulnerable communities that CNCS programs serve; and (2) the real risk that dangerous offenders could use national service to gain access to easily exploited individuals. Expanding the practical assistance provided to grantees—education about red flags and warning signs, suggested policies and other ways to protect their communities—will help to minimize the risk of harm to individuals and ensure the safety of CNCS-funded programs.

## More robust enforcement

The goal of CHC enforcement is to incentivize compliance and reinforce the importance of properly screening national service members and staff, relative to other priorities. To accomplish these ends, enforcement must be predictable, consistent and commensurate with the risk of harm.

CNCS recently adopted a series of small fines as sanctions for CHC noncompliance. Consistent accountability represents important progress. In other respects, however, the enforcement regime should be strengthened, to match the gravity of the consequences to vulnerable individuals, to grantees and to CNCS itself if noncompliance were to allow a violent predator to harm an at-risk person in a CNCS program. Improvements are needed to align the sanctions to the risk of harm and to ensure that grantees make safety their top priority.

To create meaningful incentives, the fines — currently as low as $750 for enrolling a member without any background check and $250 for a partial or grossly untimely check— must be higher.5 Most noncompliance goes undetected because CNCS visits only a fraction of the grantees in any given year and does not directly monitor subgrantees, where the majority of AmeriCorps members serve. A small risk of a small fine may cause a grantee to dismiss the sanctions as a minor cost of doing business. The nominal amounts undermine CNCS's messaging that background checks should be a high priority.

The sanctions are also disproportionately small relative to the cost disallowances by which CNCS routinely enforces non-safety-related regulatory requirements. Perversely, grantees

[5] A $250 fine befits a minor regulatory infraction; unauthorized parking on private property carries a fine of $250 in the District of Columbia, and the fine for failing to recycle is almost as high. During the period March 1 — August 31, 2016, the median sanction was only $1,500, on average less than one percent of the funding that the grantee received from CNCS.

may find it more cost-effective to direct their limited resources to timekeeping, expense receipts and fundraising for match, rather than to protecting vulnerable people from violent predators. That is clearly not what CNCS intended.

Changes are also necessary to make the sanctions truly risk-based. The current sanctions regime in some instances levies substantially different penalties for identical risks to the public. In other instances, it imposes the same penalty for vastly different risks. Some of its features burden small grantees more than large grantees for the same noncompliance. It also rewards grantees unduly for being lucky, even though Congress required specific CHCs precisely to preclude grantees from relying on luck to manage this risk.

## Management Challenge 3: Reducing Improper Payments

Improper payments—payments that should not have been made, are unsupported by documentation or were made in incorrect amounts—present a continuing challenge to the effective use of taxpayer funds throughout the Federal government. Without a means to prevent, identify and reduce improper payments, government agencies must instead divert their time and resources to attempting to recover funds, leaving the public to bear the costs and risks associated with that "pay and chase" approach.

According to a recent report from the Government Accountability Office, improper payments across the government since 2003 may exceed $1 trillion. CNCS represents only a small fraction of that total, but the extraordinarily high level of improper payments that it has reported for FY 2016, coupled with its inability to meet the government-wide standards for quantifying those payments, leaves it unable to assure taxpayers that their funds are being spent properly. For years, CNCS has struggled unsuccessfully to determine which of its programs and activities are at risk of more than $10 million in improper payments annually, to detect improper payments in programs deemed to be susceptible, to estimate and report the rate and amount of those improper payments, and to reduce and recapture them. By law (the Improper Payments Elimination and Reduction Act of 2010, as amended, known as IPERA), CNCS must report annually on the amount and rate of improper payments in any program susceptible to more than $10 million in such payments annually.

CNCS-OIG's annual evaluations have consistently found significant flaws at every stage of the agency's IPERA process. As with many of the challenges that dog grants management and monitoring, CNCS lacks sufficient expertise and has never devoted the level of resources necessary to analyze the issues or to develop and execute proper sampling and testing to detect improper payments. CNCS has made progress over the last four years,[6] but the agency still lacks an effective strategy to assess, reduce, recapture and report on improper payments across the agency.

For FY 2015, CNCS quantified the necessary information for only one program, AmeriCorps State and National (ASN). The results were startling. According to CNCS, ASN made an estimated $14.5 million of improper payments, representing 6.5 percent of its total expenditures. Because, as CNCS-OIG found, these results were not statistically valid, complete or accurate, the actual figures might have been higher. CNCS could not produce estimates for the Foster Grandparents Program (FGP) and RSVP, each of which it had determined to be susceptible to more than $10 million in improper payments.[7] In addition, CNCS may have underestimated the susceptibility of the Social Innovation Fund and the Senior Companion Program (SCP) to improper payments, calling into question their omission from IPERA analysis. CNCS acknowledged forthrightly that it had not complied with IPERA and promised a number of improvements, detailed in its Agency Financial Report for FY 2015. Unfortunately, CNCS lacked the capability to execute its promises and did not achieve compliance in FY 2016. Delays, an absence of leadership for most of the year and a decrease in resources contributed to this result. Due to poor sample planning, CNCS could not determine either the rate or the amount of improper payments in ASN. Based on a limited FY 2016 sample, CNCS reported an extraordinary level of improper payments in the three Senior Corps programs: 34 percent for FGP; 23 percent in RSVP and 33 percent in SCP. All told, this represents improper payments totaling $ 47 million, 30 percent of Senior Corps' outlays.

The Office of Management and Budget has directed CNCS to develop more precise estimates for FY 2017 and to submit a plan for doing so. Realistically, however, it may be two years or more before CNCS manages to meet its obligations under IPERA.

[6] In its FY 2011 Agency Financial Report (AFR), CNCS estimated that it made less than $4,000 in improper payments, a result inconsistent with OIG audit findings and not credible on its face. The FY 2012 assessment relied on stale information and excluded from its analysis grantees' use of approximately $ 750 million in grant funds, representing 75 percent of the agency's budget. In its FY 2012 AFR, management promised to complete a new statistical analysis of payments within each of its programs in FY 2013, perform a new risk assessment, quantify the results for the AmeriCorps State and National Program (ASN) and report the results in the FY 2013 AFR. CNCS was unable to live up to these commitments in 2013, and promised again to fulfill them in 2014. That year, CNCS concluded that ASN, the Foster Grandparents Program (FGP) and RSVP are each susceptible to more than $10 million of improper payments annually, but could provide an estimate only for ASN, which it estimated to have made $12.4 million of improper payments. OIG found a number of fundamental flaws in the analysis, and we recommended that it be re-performed *ab initio* the following year.

[7] CNCS continued to employ a sampling and testing methodology that had proven unsuccessful in the past and which it lacks the resources to execute. CNCS-OIG recommended that CNCS either abandon that approach in favor of an alternative that can be timely executed with the available resources, or marshal sufficient additional resources to bring this methodology to completion, working with Congress and OMB if necessary.

Far more than money is at stake. The overwhelming majority of improper payments identified at CNCS stem from grantees' failure to complete timely and thorough criminal history checks (CHCs) for national service participants and grant-funded staff. *See* Management Challenge 2. The IPERA process has been the Corporation's principal tool for gauging the level of compliance with this critical safety measure. Without a reliable, repeatable process, CNCS has no way of knowing whether its efforts to improve compliance are effective.

Making better use of the information derived from the IPERA process is another critical challenge. CNCS did not begin efforts to recover the improper payments identified in 2013 and 2014 until late in FY 2016. Moreover, many of its programs did not incorporate the information into their risk assessments, either for those grantees that made improper payments or those that failed to respond the agency's information requests.[8] The IPERA data also revealed substantial discrepancies between certain grantees' internal accounting records (general ledger) and the expenditure reports that they submitted to the Federal government (Federal Financial Reports, or FFRs). Such discrepancies suggest a possible misapplication of Federal funds. If a grantee cannot and does not routinely reconcile these records, then its capability to manage Federal funds is called into serious doubt. CNCS did not pursue these matters with the grantees.

## Management Challenge 4: Securing Information Systems and Modernizing Information Technology

### Securing Information Systems

Safeguarding data and information systems poses a continuing challenge throughout the Federal government, including at CNCS. The theft of an estimated 22 million Federal personnel records from the Office of Personnel Management (OPM), and the high cost of protecting those individuals from identity theft, illustrates the high stakes of information security. Privacy, as well as information security, continues to be a concern. The Government Accountability Office (GAO) has identified the protection of cyber assets and the privacy of personal data as high-risk areas.[9]

[8] For FY 2015, CNCS described "the agency's substantial nonresponse rates across programs, which resulted in CNCS's failing to test enough samples to reach the required statistical confidence interval . . . ." In other words, grantees did not cooperate with requests for information, making it impossible for CNCS to complete its work. That high nonresponse rate is itself cause for concern. CNCS stated that its poor communications with grantees contributed to the high level of nonresponse.

[9] See http://www.gao.gov/highrisk/ensuring_the_security_federal_government_information_systems/why_did_study

Six of CNCS's information systems of record contain personally identifiable information (PII). This includes the names, dates of birth, email addresses and Social Security numbers of current and former CNCS staff and of members of AmeriCorps State and National, VISTA and the National Civilian Community Corps. Some of the systems include the PII of family members and the names and locations of their childcare providers. Certain systems contain bank account numbers and records of financial transactions. Because CNCS provides healthcare coverage for national service members, two of its information systems contain protected health information, including diagnoses, treatment, provider names and medical claims.

Without adequate management, operational and technical security controls in place, CNCS’s systems and information are vulnerable to attack, whether from outside or by insiders. Unauthorized access could result in losing data confidentiality and integrity, limiting system availability and reducing system reliability. CNCS has experienced first-hand a consequence of inadequate security; a ransomware attack in 2016 prevented many users from accessing network systems for 16-34 hours. Although CNCS was able to restore data from its backup tapes, staff lost significant work time while the system was unavailable.

CNCS’s IT security has suffered from many of the same defects that allowed the breach at OPM. Over the last few years, IT security audits and evaluations have identified substantial vulnerabilities. These deficiencies were so severe that CNCS was required to disclose them publicly in its Agency Financial Reports for FYs 2014 and 2015 as a material weakness. They included failure to remedy known vulnerabilities (including the failure to apply available patches), ineffective vulnerability scanning, limited identity and access management, delayed incident response and reporting, lack of a risk management framework, lack of data loss prevention tools, and absence of continuous monitoring.

With strong leadership support since FY15, CNCS has made large investments to strengthen its IT security program, including measures to develop secure baseline configurations, a clear process to update software across the Corporation’s servers, and studying the use of data loss prevention tools and technology to monitor, detect and block sensitive data from unauthorized use. These investments are beginning to pay off. For the first time in three years, the FY 2016 information security audit did not find a significant deficiency. Auditors found that CNCS has fully resolved eight of the 17 prior-year findings and closed 67 of the 90 recommendations. CNCS’s information security risk management and continuous monitoring have also improved, though further work is needed to make them effective. Following the ransomware attack, CNCS improved its patch management and antivirus monitoring of all devices and began a migration to a SharePoint architecture that will also better protect PII.

Vulnerabilities remain, however, and sustained effort will be required to mature CNCS's information security program to an effective level. A risk-based approach to IT security and privacy, including multi-factor authentication (PIV cards) to control access to information systems by privileged and nonprivileged users, automated and centralized continuous monitoring, and implementation of configuration management policies and procedures, will better equip CNCS to prevent, detect and respond to attacks or incursions. In addition, CNCS must keep pace as threats evolve, new risks emerge and the use of technology changes.

## Modernizing Information Technology

CNCS's legacy information technology for grants management does not support robust oversight. An evaluation performed by MITRE Corporation in 2014 confirmed that the IT infrastructure does not meet the current or future needs of the Corporation's programs and does not provide reliable data to inform management's key decisions. Among the highlights of this dismal picture:

- There is a substantial and widening gap between the services that the Office of Information Technology (OIT) can currently provide and the increasing business needs of CNCS's expanding mission, greater regulatory and reporting demands and faster operational tempo;

- Current IT assets do not support evidence-based decision-making by CNCS management;

- The IT system does not reliably produce consistent and valid information; assembling basic information requires staff to spend considerable time looking for, compiling and validating information from many sources;

- The IT system cannot provide data analytics, a basic and increasingly important management tool for comparing performance, identifying patterns and trends, and minimizing fraud and waste;

- CNCS was spending 28 percent less per employee on IT than other federal agencies and 42 percent less than financial institutions. 98 percent of OIT's budget was devoted to Operations and Maintenance, which MITRE described as "keeping the lights on," leaving little or no funding to improve or meet new needs; and

- The customized and outsourced IT solutions chosen by CNCS in the past are unduly complicated and expensive and inhibit the Corporation from changing vendors.

CNCS has since adopted and begun to implement a new Grants and Member Management Modernization program (GMM). According to CNCS, the GMM modernization will enhance business agility and program effectiveness, improve data quality, timeliness and accessibility and increase staff productivity. The Corporation has engaged contractors and is using an "agile" (vs. a waterfall) project development process.

The modernization effort is expected to cost approximately $43 million. It is by far the largest IT investment since the creation of CNCS.

GMM began in FY 2014 and consists of three phases:

Phase 1 – Grants Management: Stand up a highly configurable platform. Individual projects include grants planning through the Notice of Funding Availability, review of grant applications, grant funding packet routing, grantee and project reporting, and grant and project closeout.

Phase 2 – Member Management: Key projects include member recruitment and acceptance, onboarding and off boarding, training and orientation, member travel, member payroll management, as well as management of awards from the National Service Trust.

Phase 3 – Performance Measures and Analytics: Key projects include performance measures, data analytics, new mobile applications and services, as well as and customer contact relationship management, to be followed by sunset of CNCS legacy systems.

Phase 1 was originally scheduled for completion in May 2016 but has been twice delayed, in part because of contractor nonperformance. Its anticipated release date is now October 2017. CNCS has obligated $20 million for Phase 1 and reports that it has already expended $13.9 million, or 70 percent of the obligated funds, with the now-delayed delivery one year away.

No target dates have been established for deployment of Phases 2 and 3. Until that occurs, CNCS must continue to operate, rely on and invest in its deficient legacy systems. And, until the unknown future date when data analytics will be available, CNCS will remain unable to automate routine monitoring tasks, benchmark and perform other comparisons necessary for robust grant oversight. Moreover, the original intent was to design Phase 1 in tandem with developing a new grant risk model, a task that CNCS put aside in FY 2015 for lack of in-house capability. Work on that new risk model has not yet begun, and the staff member hired to lead that effort has just reported for duty.

Effective operation of CNCS's core business depends heavily on successful and prompt completion of GMM, which is far from assured. Studies of major IT development projects consistently show a high rate of failure. GAO recognizes IT acquisitions/development as a high-risk area, observing that "federal IT investments too frequently fail or incur cost overruns and schedule slippages while contributing little to mission-related outcomes." Such projects often "lack [] disciplined and effective management, such as project planning, requirements definition, and program oversight and governance" and because the agency "ha[s] not consistently applied best practices that are critical to successfully acquiring IT investments."[10] GAO has recently begun a study of CNCS's GMM project, but it will be some time before the results become available.

CNCS has no track record of managing projects of this complexity and magnitude. Given this inexperience, the urgent need for better IT to support grant management, the amounts at risk, the delays to date, the expenditure of one-third of the total estimated cost long before completion of Phase 1, and the lack of any planned delivery dates for Phases 2 and 3, careful management and close executive oversight will be necessary to bring this critical project to a successful completion. The dire picture of CNCS's existing IT systems painted by the MITRE study and the concerns about this project expressed by Congressional oversight authorities further raise the stakes.

## Management Challenge 5: Rethinking the Fundamentals to Support National Service

CNCS operates much as it did 23 years ago, when programs of different origins were cobbled together to form the Corporation. The intervening two decades have seen substantial changes in the nonprofit sector and across the Federal government. Re-examination of CNCS's fundamentals—agency structure, priorities, programmatic investments and administrative support functions—is due. If national service is to prosper, CNCS's now-overstretched capacities must grow.

In a constrained budget environment, government agencies face considerable pressure to maximize the efficiency of their internal operations as they strive to "do more with less." The need is particularly acute at CNCS, where historic underinvestment in personnel and infrastructure, coupled with increasing demands and rising standards, requires rapid improvement across the agency.

Incoming and current CNCS leaders should consider a radical restructuring of CNCS and its programs, based on the best way to engage the public and provide services to communities in need. This is an opportunity to redesign CNCS. No expert, if given a free hand to achieve

[10] *See* http://www.gao.gov/highrisk/improving_management_it_acquisitions_operations/why_did_study

CNCS's mission on an operating budget of $1 billion per year, would choose the constraints, redundancies and Byzantine structure that characterizes CNCS and its programs.

At its most fundamental, this redesign could include merging some or all of the programs into a single unit, with a single budget. This would give CNCS's leaders the flexibility to direct programmatic resources according to current and emerging priorities and the option to make quick investments into urgently needed infrastructure upgrades, rather than allow problems to fester until the next budget cycle. It would also place all of the current programs under the same set of administrative rules and regulation, rather than the mosaic of small differences that now exist. Any such proposal should include a serious effort to simplify program requirements and to remove or reduce administrative burdens that contribute little to program safety, success or oversight. Changes this fundamental would require comprehensive legislation, a long and uncertain process.

While pursuing comprehensive legislation, CNCS leaders should also seek smaller changes, including through the budget process, and use their existing authority to streamline and rationalize operations. Elements of that change could include:

1. Rebalancing the allocation of resources among programs to serve communities more cost-effectively

Expensive program models, such as the National Civilian Community Corps (NCCC), should be reserved for service activities that they can perform in a cost-effective manner. Tutoring, tax assistance, maintaining hiking trails for recreational use, and many other activities that form the bulk of NCCC hours can be performed equally well at a fraction of the cost by CNCS's non-residential programs. Even disaster response services can be provided more cost-effectively by AmeriCorps Disaster Response Teams (A-DRTs), AmeriCorps State and National (ASN) grantees with the same specialized training as NCCC. Senior Corps grantees and ASN grantees that do not have A-DRT training also participate actively in disaster response and recovery work.

NCCC costs four times more per member than ASN. This higher per-member cost, and the five residential campuses that it supports, do not have a substantially greater measurable impact on members. To the contrary, ASN alumni achieve outcomes comparable to alumni of NCCC, according to two recent research studies sponsored by CNCS.

By shifting member slots from NCCC to ASN, CNCS can multiply the services to communities and the number of individuals who can participate in national service, with little or no increase in cost. Like NCCC, many ASN programs focus on enrolling youth from disadvantaged circumstances and provide training to develop soft career skills and civic engagement. Expanding and increasing the capabilities of the A-DRTs, and cultivating new ones, can expand critically needed disaster response and recovery capacities.

For an in-depth exploration of this issue, see Report No. 17-05, *Evaluation of the AmeriCorps National Civilian Community Corps Program*, available at http://www.cncsoig.gov/news-entry/17-05.

2. Consolidating financial and/or programmatic oversight

CNCS employs a hodgepodge of centralized and decentralized oversight models. ASN has a hybrid structure, with certain grants awarded competitively and monitored programmatically by the AmeriCorps Program Office (APO) in CNCS's headquarters. The Office of Grants Management (OGM), also located at headquarters, is responsible for financial management of ASN grants. The majority of ASN funds, however, are distributed and overseen through State Commissions, subject to limited oversight by APO and OGM.

The Senior Corps Programs are led from Washington, DC, and funded through formula grants. The Office of Field Liaison (OFL), with staff in State Offices throughout the United States, conducts their programmatic supervision. Financial oversight was originally decentralized, but was ultimately consolidated into the Federal Financial Management Center (FFMC) in Philadelphia, PA. VISTA also follows this model.

Whether CNCS is best served by maintaining two oversight models for ASN, plus a separate oversight system for Senior Corps and VISTA, is a question worth exploring. Consolidating the two financial management operations into a single office with uniform processes could streamline this function, eliminate redundancies and facilitate comprehensive management of the grant portfolio.

There are at least three options for CNCS leaders to consider with respect to programmatic oversight of Senior Corps:

a. Consolidating OFL into the Senior Corps Program Office: The creation of OFL as an entity distinct from the Senior Corps Program Office appears to be a historical artifact, a compromise struck 20 years ago for reasons no longer extant. For the last year, OFL and Senior Corps have operated under common Acting leadership. Uniting the field offices into Senior Corps would enable program leaders to better understand and manage their program risks.

b. Tasking the State Commissions with programmatic oversight of Senior Corps: Maintaining two decentralized oversight structures, one for ASN and another for Senior Corps, seems wasteful. Expanding the ASN State Commission structure to include oversight of Senior Corps programs might offer economies of scale and expand the available capabilities.

c. Centralizing Senior Corps' programmatic oversight: While a decentralized structure gives program officers more opportunities to observe and assist grantees, it also carries significant downsides. Given the small size of many Senior Corps grants, onsite oversight may not be warranted under a risk-based approach to grant monitoring. Increased use of fixed amount grants for small awards could also simplify monitoring.[11] As CNCS upgrades its grant management information technology and develops data analytics capabilities, a field presence becomes even less necessary. Taken together, consolidating this function at headquarters could reduce the workforce necessary to monitor the Senior Corps programs, freeing those resources for other uses.

Centralized monitoring may also be more objective, because it would enable routine rotation of grant portfolios. *See* Management Challenge 1. There is very little turnover in the Senior Corps grantee population, increasing the risk that program officers will develop personal relationships with grantees that affect their independence. They may come to view the grantees as their clients, and the assistance role may crowd out their oversight and accountability obligations. Greater objectivity would support more accurate comparisons.
Certain issues may be sufficiently important for CNCS to monitor them directly and on a consolidated basis, across programs. The Chief Risk Officer could, for example, take responsibility for oversight of safety requirements, such as criminal history checking, or prohibited activities, violations of which have twice led to Congressional oversight hearings.

3. Aligning VISTA and ASN

The natural synergies and similarities between VISTA and ASN suggest that VISTA oversight should be performed in tandem with ASN rather than with Senior Corps. The VISTA program is making increasing numbers of grants to sponsors, as well as funding member stipends. Under Operation AmeriCorps, an increasing number of grantees participate in both VISTA and ASN. Most ASN grantees share VISTA's anti-poverty mission, and many of them could use VISTA's capacity-building assistance. Aligning the grant award, management and oversight

[11] For example, RSVP grants average $75,000. Though SCP and FGP grants average more, $200,000 and $300,000, respectively, both programs award a number of small grants. Given the formula-based awards, the modest amounts and the difficulty in effective monitoring, CNCS leaders should consider whether to recommend that the Senior Corps programs be converted to block grants, perhaps leaving at CNCS the option to award large grants on a competitive basis, as in AmeriCorps National Direct grants.

processes of the two programs may therefore be advantageous. By doing so, CNCS may get many of the benefits of merging the programs functionally, while retaining the separate identity and rich history of the VISTA program.

This alignment would also support the transition to monitoring by grantee, rather than by grant. Currently, an organization with funding from multiple CNCS programs is subject to oversight by each, no matter how duplicative. Worse, the programs do not share grant risk analyses or oversight information. CNCS-OIG recently cited an instance in which VISTA awarded resources to an organization on the day after ASN terminated its grant because the organization refused to cooperate with information requests. *See* CNCS-OIG Audit Report No. 15-05, *Audit of Corporation for National & Community Service Grants Awarded to Tufts University Massachusetts Campus Compact*, at http://www.cncsoig.gov/sites/default/files/15-05.pdf.

As part of this realignment, CNCS should consider standardizing its grant application and award processes. Currently, a grantee that receives funding from multiple Corporation programs must file separate applications, each with its own information requirements; there is no universal form. Allowing grantees to apply for funding and other resources from multiple programs in a single application will reduce the burdens on grantees and streamline the award process. It will also allow CNCS to make comprehensive, cross-program decisions about the most effective deployment of resources.

4. Improving back office operations through shared services

Among other infrastructure challenges, CNCS has experienced ongoing problems in attracting, training and retaining staff in critical support functions, such as accounting and contracting. The Corporation’s small size and its static compensation (no annual step increases as at other agencies) create a serious competitive disadvantage. Turnover has been costly and disruptive, leading to delays and performance weaknesses that CNCS can ill-afford.

CNCS leadership should consider outsourcing some of these administrative support functions via shared services agreements. While this necessarily involves some loss of autonomy, it will reduce the burdens on overtaxed management and should increase the quality and timeliness of service and the controls to which these functions are subject.