Statement of Deborah J. Jeffrey, Inspector General
Corporation for National and Community Service

before the United States House of Representatives
Committee on Education and the Workforce
Subcommittee on Higher Education and Workforce Development

March 28, 2017

Chairman Guthrie, Ranking Member Davis, and Members of the Subcommittee:

Thank you for the opportunity to testify today about the work of the Office of Inspector General (CNCS-OIG) to strengthen grant oversight and accountability at the Corporation for National and Community Service (CNCS or the Corporation). As you know, the OIG is an independent and nonpartisan unit charged with detecting and preventing waste, fraud and abuse and improving the efficiency and effectiveness of CNCS and its programs. I have had the privilege of serving as the Inspector General for nearly five years.

Grant-making is CNCS's core activity, and grants account for three-quarters of the Corporation's annual budget of $1 billion. At any given time, CNCS must oversee more than 2,100 active grants, ranging in size from $40,000 to $10 million, in seven programs that operate throughout the United States, its Territories and Indian Tribes. Grantees include well established national nonprofits, such as the Red Cross, major research universities, State and local governments and small community-based organizations that depend on CNCS for the majority of their funding. Not surprisingly, these grantees vary greatly in their capabilities, experience and infrastructure. All of this presents challenges for grant oversight.

Today, I would like to update the Subcommittee on developments in CNCS's grant oversight since my last appearance. In addition, my testimony will describe the significant challenges that remain and explain how CNCS can meet them.

Positive Developments

of the Chief Risk Officer. Over the past four years, CNCS-OIG warned repeatedly that CNCS lacked the skilled leadership and experienced staff needed to

Standing up the Office strengthen internal controls and risk management, and that these critical areas were severely under-resourced. The past year has seen dramatic improvements in this area. In April 2016, CNCS created the Office of the Chief Risk Officer (OCRO) at the executive level and hired my co-panelist, Lori Giblin, an experienced risk management professional, as its leader. OCRO is now responsible for areas that have historically proven challenging for CNCS: criminal history checking, identifying and reducing

improper payments, improving grant risk management, introducing Enterprise Risk Management to CNCS, and the testing and improvement of internal controls.

Based on her needs assessment, the Office of the Chief Risk Officer now employs 17 staff members, with additional funds available to engage contractors, to support the rapid improvements that CNCS's leadership now recognize to be necessary. The oversight of this Subcommittee, statements accompanying appropriations bills in the House and Senate and the support of the Office of Management and Budget (OMB) were essential in persuading CNCS to devote this level of support to OCRO.

Strengthening the Office of Grants Management. The Office of Grants Management (OGM) provides critical financial oversight of grants and is responsible for recovering misspent funds. CNCS-OIG has seen both cultural changes and increased capacity in this area.

Bringing in leaders with substantial grant management expertise from other Federal agencies has created a more business-like and rigorous approach to financial accountability. OIG has observed greater willingness to hold grantees to grant terms and conditions, disallow improperly incurred costs and recover the funds promptly.

CNCS has expanded the capacity of OGM by 43 percent, restoring staffing to the level needed for effective oversight. To cite one example, CNCS-OIG reported in 2016 that, although the Social Innovation Fund (SIF) had made grants then totaling some $241 million, its entire grant portfolio was overseen by a single senior grant officer, who also had other supervisory responsibilities. CNCS now devotes three grant officers to oversight of the SIF.

OGM's increased capacity has produced immediate results. OGM has eliminated its backlog of management decisions and corrective actions on OIG audits and investigations. Increasing the timeliness of corrective actions and collection of disallowed costs improves accountability and reduces the vulnerability of particular grants. The expectations and messaging communicated by OGM to grantees support strong accountability.

More sophisticated approach to internal controls. Under OCRO's leadership, CNCS has assessed risk across 19 business processes and are beginning meaningful compliance testing in the areas determined to be high-risk. These include procurement, purchase and travel cards and accounts receivable. This represents significant progress in an area repeatedly found to be weak in the Corporation's prior annual financial statement audits.

Stronger cybersecurity. For years, our audits found significant deficiencies in the security of CNCS's information technology sysems. Over the last 18 months, the Corporation invested heavily in this area, and our 2016 cybersecurity audit reported substantial improvements. We no longer consider CNCS's IT security to be significantly deficient, and CNCS was not required to report a material weakness in cybersecurity in its annual report.

Though further work is needed to achieve full effectiveness, the progress in cybersecurity shows that CNCS can leap forward when it focuses its efforts.

Continuing Management Challenges

Strengthening grant risk management. To manage its extensive grant portfolio effectively and efficiently, CNCS must develop and implement risk-based grant management. This is the most critical challenge confronting the Corporation and is the single most important recommendation of CNCS-OIG that CNCS has not yet implemented.

Instead, CNCS continues to operate today under most of the same monitoring protocols that my Office has found to be poorly designed and implemented. For example, routine grant monitoring failed to detect:

- **Fraud** – Leaders of the national service program in American Samoa used national service funds to entertain themselves with lavish personal travel. They also bilked the taxpayers by charging inflated rents for broken down shacks owned by family members and falsely claiming that national service programs were operating from those locations. CNCS personnel conducted site visits annually while these frauds were occurring, but never discovered them.

  A community college claimed that its students were performing $4 million worth of community service when those students were merely completing the classroom study and clinical work required for their degrees. The $4 million expenditure provided no net benefit to the community.

  Perhaps it is not surprising that CNCS's grant monitoring does not discover such frauds, because the monitoring protocols contain few, if any, fraud prevention and detection measures. Until recently, leaders did not acknowledge that the Corporation's programs are subject to fraud risk and therefore did not identify, assess and mitigate those risks.

- **Widespread inadequacies grantees' performance of statutorily required criminal history checks intended to exclude murderers and sex offenders from national service** – According to the Office of the Chief Risk Officer, between 22 and 41 percent of grantees do not conduct thorough and timely criminal history checks, potentially jeopardizing the safety of the communities served by CNCS programs.

  This risk is more than theoretical. Last week, my Office learned that a volunteer who had been convicted of three sex offenses served for more than one year in the Senior Companion Program, which works with the elderly in their homes. In 2013, we found a murderer and a sex offender working on a subgrant funded through the Social Innovation Fund. Instead of removing them when it learned of their criminal histories, the subgrantee allowed them to continue to work on the grant-funded program but paid their compensation with other funds. CNCS-OIG discovered this in an audit. On

the other hand, careful compliance by an AmeriCorps grantee last year enabled the organization to exclude a convicted sex offender shortly after he began serving.

At one Senior Corps grantee, investigators discovered that more than 120 individuals were serving without proper criminal history checks.

CNCS is doing more to find noncompliance and enforce the rules, but, as I discuss later in this statement, the problem is far from solved.

- **Prohibited activities** – CNCS rarely learns of prohibited activities[1] through its routine grant monitoring. Instead, the information typically comes from self-reporting by a grantee, a whistleblower call to the OIG hotline, or discovery in the course of investigating other allegations. As I testified ten months ago, CNCS does not currently identify grantees that are at risk of specific prohibited activities, nor does it have appropriate techniques to monitor those grantees' compliance.[2]

  Last year's hearing arose from an investigation that found a major grantee to have allowed a subgrantee to violate the prohibition on using AmeriCorps resources for "abortion services or referrals for the receipt of such services." 42 U.S.C. § 12584a(a)(9). CNCS-OIG recommended that CNCS explain clearly, definitively and transparently how it will interpret and apply this prohibition. Without such an explanation, program officers may provide incorrect and inconsistent direction to grantees, who remain unnecessarily at risk of violating the law, with severe consequences.

  In December 2016, CNCS's Office of General Counsel (OGC) prepared a written analysis of the abortion prohibitions. This is the first time that CNCS has reduced to writing an explanation of the restrictions and how they are to be applied.

  In other respects, however, CNCS has not implemented CNCS-OIG's recommendations.[3] OGC's advice was not transparent and has not been released to the general public. The AmeriCorps program has not translated the legal analysis into practical guidance for grantees, members and program officers. CNCS has not determined whether non-healthcare grantees may also present a heightened risk of abortion-related prohibited activities. Both logic and experience indicate that

[1] The national service laws forbid the use of national service resources for eleven categories of activity, including legislative advocacy; partisan and political activity; religious study, worship and proselytizing; strikes, boycotts and protests; pro- or anti-union organizing; abortion services and referrals; and supporting a for-profit business or organization. 42 U.S.C. § 12584a.

[2] For more detail, see *Special Review: Prohibited Activities: Missed Opportunities, Red Flags Ignored and Next Steps to Improve Grants Management at CNCS* (Dec. 21, 2016) at https://www.cncsoig.gov/sites/default/files/nachc_missed_opportunities.pdf.

[3] CNCS also needs to determine which of its grantees present a heightened risk of other prohibited activities. Faith-based groups, for example, face a higher risk of religious worship, study or proselytizing than do secular groups. 42 U.S.C. § 12584a(a)(7). Grantees associated with for-profit entities are more likely to run afoul of the prohibition on providing a direct benefit to such an organization. 42 U.S.C. § 12584a(a)(8)(A). CNCS has not implemented our recommendation to conduct such a risk analysis.

grantees serving children and youth and those serving immigrant populations are also points of contact for girls and women facing crisis pregnancies.

CNCS also needs to develop better methods of detecting prohibited activities when they occur. Currently, CNCS monitors for prohibited activities by interviewing members during site visits. But those site visits may occur only once every six years, and they include only a fraction of subgrantees and service sites. CNCS has not implemented CNCS-OIG's recommendation to develop surveys that will enable more frequent contact with members.

The shortcomings in CNCS's approach to prohibited activities illustrate the need for a disciplined, risk-based approach to all aspects of grant making, management and monitoring. There is a significant opportunity to improve stewardship, cost-effectiveness and results by strengthening the way that CNCS ***assesses*** grant risk and the way that it ***monitors and manages*** those risks.

Currently, CNCS decides annually which grants it will monitor closely by assessing each grant according to a uniform set of 19 criteria, which it treats as risk indicators. It uses the same criteria across the entire agency, despite critical differences among CNCS programs and grant vehicles that bear directly on risk. The model omits significant risks identified in CNCS-OIG audits and investigations, and it includes no fraud indicators. (No one currently at CNCS can explain how the criteria were selected or why they are weighted as they now are.) CNCS uses this model to calculate a single risk score; a grantee that scores in the "high" range typically receives a site visit from a program officer, who goes through standardized steps prescribed by a "monitoring tool."

As I told the Subcommittee 10 months ago, CNCS relies heavily on this model, but has never validated it against outcomes. The entire grant monitoring program still rests on assumptions that are untested. CNCS-OIG audits and investigations often uncover major problems at grantees that the Corporation rated as low or medium risk and therefore did not scrutinize closely. To take one example, a grantee rated as low-to-medium risk ceased operations and went bankrupt during the grant, owing CNCS over $1 million. A preliminary analysis by CNCS-OIG of grants with catastrophic outcomes—filing for bankruptcy during a grant, ceasing operations mid-grant, or CNCS terminating the grant for cause—showed that half were rated as low or medium risk. A risk model that fails to warn of an impending catastrophe 50 percent of the time isn't much good. CNCS has operated under this risk model for about ten years, with only modest tweaks along the way.

Now that CNCS has an experienced Chief Risk Officer, supported by a robust staff and budget, it has the capacity to develop a more granular approach to risk. Doing so will enable CNCS to direct its limited resources (grant funds and staff attention) where they will have the greatest impact. Achieving risk-based grant management will require the following steps:

1. Identifying the risks associated with various kinds of grants and grantees, including fraud risk. Key question: what events or factors could impact performance, compliance and financial management of a grant?;

2. Developing indicators that align to those risks. Key question: how could CNCS know whether those events and factors are likely to exist?;

3. Assessing the individual risks presented by each grantee. Key question: what is the likelihood and potential impact of each of these risks?

4. Mitigating risks. Key question: what could CNCS or the grantee do to reduce the likelihood that a risk will materialize or its impact?; and

5. Developing oversight activities suited to particular risks. Key question: what is the most cost-effective way to monitor for the risk in question?

The resulting risk model should inform every aspect of grant management throughout the grant lifecycle, including the information elicited in grant applications, whether to impose special conditions on a particular grant and selecting the appropriate monitoring activities.

Risk does not exist in the abstract; when we say that a grantee is high-risk, it is at high risk of *something*, a particular failure, problem or bad outcome. By breaking grant risk into its component parts—financial, programmatic, compliance, etc.—CNCS can target its monitoring on the specific component or activity within a grantee that is high-risk. A grantee that presents a significant financial risk needs to be monitored for that risk, even it is low-risk in other respects. This would represent a significant improvement over the current single risk score and site visit approach, which is both underinclusive and overly broad: (1) underinclusive in that a grantee may present a high financial risk but escape monitoring if its overall risk score falls into the low or medium range; and (2) overly broad because a grant that scores in the high range will undergo the full range of site visit monitoring activities, even those that address risks that are *de minimis* for the particular grantee. Breaking grant risk into its component parts will make CNCS's monitoring more precise and effective and less wasteful.

Risk-based grant management may also require changes to the CNCS's workforce and organizational structure. The type of risk presented should dictate who performs the monitoring. Where financial risks predominate, grant officers, who have extensive financial training, should conduct the necessary monitoring. Similarly, better risk assessments and risk-based monitoring may make it unnecessary for CNCS to maintain an office in every state to oversee Senior Corps grantees. Converting the smallest CNCS grants[4] to a fixed-amount basis would simplify financial administration for the grantees and reduce the amount of oversight needed.

[4] RSVP grants average $75,000. Though the Senior Companion Program and the Foster Grandparent Program grants average more, $200,000 and $300,000, respectively, both programs award a number of small grants.

CNCS should also monitor by grantee, rather than by grant, as it now does. An increasing number of grantees participate in multiple CNCS programs, and those programs should be pooling information about grant risks. In 2013, VISTA made an award to a grantee one day after AmeriCorps terminated its relationship with the same grantee, because it refused to cooperate with corrective actions arising from a monitoring visit. The grants management database is not readily searchable by grantee, only by grant, so VISTA had no practical way to know that AmeriCorps found this grantee uncooperative.

Strong risk management also requires a culture of continuous improvement. CNCS should institutionalize a structured process to determine the root causes of bad outcomes, including how they could have been prevented or detected sooner. Doing so would help to identify systemic gaps, develop new risk mitigation options and address human error appropriately. A good after-action analysis creates an opportunity to learn from mistakes and to use that knowledge to refine risk assessment and monitoring, to prevent errors from recurring.

Criminal history checking. 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.[5] 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 from the Federal Bureau of Investigation (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). Audits and investigations conducted by CNCS-OIG have consistently found high rates of noncompliance. Until recently, CNCS treated them as outliers and did not recognize the pervasiveness of failure to timely screen members and staff. As I mentioned earlier in my testimony, CNCS's monitoring did not uncover the severity of this problem. Since 2014, CNCS

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

has taken a number of steps to increase compliance with this important safety measure, with limited success. In 2016, the Chief Risk Officer found that noncompliance in CNCS-funded grants ranged from 22 percent (AmeriCorps State and National) to 41 percent (RSVP). These numbers are consistent with CNCS's FY 2016 statistical analysis of improper payments.

In the past year or so CNCS has begun to enforce these requirements consistently, but its enforcement approach remains flawed. Enforcement has onsisted principally of small fines, as low as $250 for a partial or grossly untimely check and $750 enrolling a member without any background check. These amounts befit a minor regulatory infraction—parking on private property carries a $250 ticket in the District of Columbia—and trivialize the grave harm that would result if a predator were to gain access to an at-risk individual in a CNCS program. Our review of penalties for a six-month period in 2016 found that the median sanction was only $1,500, on average less than one percent of the funding that the grantee received from CNCS. These nominal amounts undermine CNCS's messaging that criminal history checking must be a priority.[6] CNCS has just announced its intention to double these fines beginning next month, but they will remain so low that a grantee might reasonably dismiss them as a small cost of doing business.

CNCS needs a better solution than expecting 2100 grantees, who experience frequent staff turnover, to check the criminal histories of tens of thousands of people each year. Given the widespread difficulties, and the resources that CNCS must now devote to CHC compliance and the related testing and recovery of improper payments, CNCS-OIG has urged CNCS to explore outsourcing criminal history checking to a vendor or vendors capable of performing the required CHCs. Doing so could radically improve compliance, relieve grantees of task that they do not perform well and enable CNCS to monitor compliance by direct contact with the vendor(s), far less burdensome than overseeing individual grantees. CNCS has agreed and charged OCRO with this responsibility. At our suggestion, the Chief Risk Officer has contacted the National Center for Missing and Exploited Children, which provided similar services to nonprofits for a number of years. The necessary contract action will take time, but it offers the best prospect we have seen to resolve this issue once and for all.

Information Technology Modernization. Following a study confirming that its legacy information technology (IT) does not support robust oversight or operating needs, CNCS has undertaken a multi-year effort to upgrade the capabilities of its grants management database and systems. Successful completion of this modernization can greatly improve the effectiveness and efficiency of grant oversight. The effort is expected to cost approximately $43 million and is by far the largest IT investment since the creation of CNCS. To date, the project has cost $19 million, and CNCS may spend an additional $6 - $7 million by the end of the current fiscal year.

[6] The risk of incurring any fine is small because most noncompliance goes undetected; CNCS visits only a fraction of its grantees in any given year and does not directly monitor subgrants. The sanctions are also disproportionately small relative to the cost disallowances by which CNCS routinely enforces non-safety-related regulatory requirements, such as timekeeping, expense recording and fundraising for match.

The modernization effort began in FY 2014 and consists of three phases:

- Grants Management (Phase 1): Standing up a highly configurable platform to integrate the entire grant lifecycle (grants planning through the Notice of Funding Availability, review of grant applications, grant funding packet routing, grantee reporting, recording monitoring results and grant closeout) into a single data system. This should facilitate seamless use of grant risk information throughout the entire lifetime of a grant.

- Member Management (Phase 2): This component includes member recruitment and acceptance, onboarding and off-boarding, training and orientation, member travel and member payroll management, as well as management of education awards from the National Service Trust.

- Performance Measures and Analytics (Phase 3): Key projects include performance measures, data analytics, new mobile applications and services, as well as customer contact relationship management.

Phase 1 is scheduled for release in October 2017, to be preceded by training for staff. No release dates or target completion dates have been established for Phases 2 and 3. Until completion of Phase 3, CNCS will remain unable to automate routine monitoring tasks, benchmark and perform other comparisons necessary for robust grant risk oversight.

CNCS's original intent was to design the new grant management database and system in tandem with developing a new risk model, a task that CNCS put aside in FY 2015 for lack of in-house capability. Consequently, these closely related efforts are not on parallel tracks, and the Office of Information Technology (OIT) does not have the new risk model to inform its development of the grant management system. OCRO and OIT have only recently begun to collaborate. Although the new system is intended to be flexible, CNCS may incur future delays and expenses in order to tailor the database to new risk management requirements.

IT acquisition/development is inherently a high-risk area, with a high rate of failure.[7] The General Accountability Office (GAO) is currently conducting a study of CNCS's IT modernization project. We do not know when it will be completed.

Let me end by saying how much I and my staff appreciate the Committee's interest in improving CNCS's grant oversight and your support of our work. Mr. Chairman, that concludes my prepared testimony. I would be pleased to answer any questions.

[7] According to GAO, "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. http://www.gao.gov/highrisk/improving_management_it_acquisitions_operations/why_did_study