C. OFFICE OF INSPECTOR GENERAL'S ASSESSMENT OF THE MANAGEMENT AND PERFORMANCE CHALLENGES FACING THE FDIC

Under the Reports Consolidation Act of 2000, the Office of Inspector General (OIG) identifies the management and performance challenges facing the FDIC and provides its assessment to the Corporation for inclusion in the FDIC's annual performance and accountability report. In doing so, we keep in mind the FDIC's overall program and operational responsibilities; financial industry, economic, and technological conditions and trends; areas of congressional interest and concern; relevant laws and regulations; the Chairman's priorities and corresponding corporate goals; and ongoing activities to address the issues involved. The OIG believes that for the foreseeable future, the FDIC faces challenges in the critical areas listed below, a number of which carry over from past years. A challenge of particular emphasis this year is *Maintaining Strong Information Security and Governance Practices*. We would point out that all of these challenges may well be impacted by changes brought on by a new Administration during 2017.

Maintaining Strong Information Security and Governance Practices

Essential to achieving the FDIC's mission of maintaining stability and public confidence in the nation's financial system is safeguarding sensitive information, including personally identifiable information that the FDIC collects and manages in its role as employer, federal deposit insurer, regulator of state nonmember financial institutions, and receiver of failed institutions. Materials that the FDIC possesses related to its Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) responsibilities contain some of the most sensitive information that the FDIC maintains and safeguarding it from unauthorized access or disclosure is critically important. Equally important to the FDIC and the Nation is the defense of critical infrastructure, which includes financial systems and associated computer network operations. In that regard, the Federal Information Security Modernization Act (FISMA) of 2014 establishes standards to assess information security government wide. The OIG's FISMA work is intended not only to ensure compliance with those standards but also to help defend the critical infrastructure against those who would attack it.

The FDIC has recently come under increased scrutiny by the Congress for specific actions it has taken related to protecting sensitive information and has been criticized for its reporting of breaches of such information, as required by FISMA and related Office of Management and Budget (OMB) guidance. The Corporation's continuing challenge will be to restore confidence both in its ability to protect the sensitive information it possesses and its actions to fully report major security incidents within prescribed timeframes, as required by law. Our office reported and testified before the Committee on Science, Space, and Technology, U.S. House of Representatives, on our work in two areas in this regard, and we continue to conduct work on related matters.

One audit dealt with the FDIC's process for identifying and reporting major information security incidents and focused on an incident where a former FDIC employee copied a large quantity of sensitive FDIC information, including personally identifiable information, to removable media and took this information when departing the FDIC's employment in October 2015. The FDIC detected the incident through its Data Loss Prevention tool. Although the FDIC had established various incident response policies, procedures, guidelines, and processes, these controls did not provide reasonable assurance that major incidents were identified and reported in a timely manner. We recommended actions to provide the FDIC with greater assurance that major incidents are identified and reported consistent with relevant guidance.

In a second audit, we reviewed the Corporation's controls for mitigating the risk of an unauthorized release of highly sensitive resolution plans. In September 2015, an FDIC employee abruptly resigned from the Corporation and took copies of sensitive components of resolution plans without authorization and in violation of FDIC policy. A number of factors contributed to this security incident. Most notably, an insider threat program was not in place that would have better enabled the FDIC to deter, detect, and mitigate the risks posed by the employee. Additionally, a key security control designed to prevent employees with access to sensitive resolution plans from copying electronic information to removable media failed to operate as intended. To address these concerns, we recommended that the FDIC establish a corporate-wide insider threat program and take other steps to better protect sensitive resolution plans. On September 20, 2016, the Corporation issued a policy formally establishing its Insider Threat and Counterintelligence Program and finalized a governance charter and implementation plan for the program.

As noted earlier, more broadly speaking, the OIG looks to its annual work under FISMA to identify the Corporation's information security successes and its ongoing challenges. Our most recent FISMA work determined that the FDIC had established a number of information security program controls and practices that were generally consistent with FISMA requirements, OMB policy and guidelines, and applicable National Institute of Standards and Technology (NIST) standards and guidelines. The FDIC had also taken steps to strengthen its security program controls following our 2015 FISMA work. Among other things, the FDIC: restricted (with limited exceptions) the ability of employees and contractor personnel to copy information to removable media in response to the major information security incidents involving the unauthorized exfiltration of sensitive information by departing employees; identified and reported its high value assets to the Department of Homeland Security (DHS); and updated its security control framework to address changes introduced by NIST guidance related to security and privacy controls for federal information systems and organizations.

Notwithstanding these actions, our FISMA audit found security control weaknesses that impaired the effectiveness of the FDIC's information security program and practices and placed the confidentiality, integrity, and availability of the FDIC's information systems and data at elevated risk. Some findings were identified during the current year and others were identified in prior reports issued by the OIG or the Government Accountability Office. Areas of notable weakness that continue to pose challenges for the Corporation include strategic planning, vulnerability scanning, the FDIC's information security manager program, configuration management, third-party software patching, multifactor authentication, and contingency planning.

The FDIC is working to strengthen the effectiveness of its information security program controls in a number of other areas. For example, the FDIC is working to improve its incident response capabilities; more effectively protect its sensitive information by improving the effectiveness of its Data Loss Prevention tool and adopting Digital Rights Management software; complete an end-to-end assessment of its information security and privacy programs; hire a permanent Chief Information Security Officer (CISO); and begin addressing action items identified during a Cyber Stat Review with OMB and DHS officials aimed at improving the FDIC's cybersecurity posture.

Other ongoing challenges for the Corporation that we pointed out involve a risk related to the performance of the vendor that supports the FDIC's infrastructure services and an observation on the frequent turnover in the CISO position and whether the CISO's authorities enable the CISO to effectively address the responsibilities defined in FISMA.

Going forward, a challenging priority for the FDIC will be to maintain effective communication with the Congress and collaboration among all parties

involved in protecting sensitive information and the Nation's critical infrastructure. Doing so will require strong leadership and an effective IT governance structure. In addition, in confronting its information security challenges, competing priorities must be carefully considered, and sound decision-making will be critical to the Corporation's success. Given the substantial financial investment in FDIC systems, security features, and related human resources, the Corporation needs to consider the cost-effectiveness and measurable business value outcomes in its decisions to fund major IT projects to ensure proper stewardship of millions of dollars in IT investments.

Carrying Out Dodd-Frank Act Responsibilities

The Dodd-Frank Act created a comprehensive new regulatory and resolution framework designed to avoid the severe consequences of financial instability. Under current law, Title I of the Dodd-Frank Act provides tools for regulators to impose enhanced supervision and prudential standards on systemically important financial institutions (SIFI). Title II provides the FDIC with a new orderly liquidation authority for SIFIs, subject to a systemic risk determination by statutorily designated regulators.

The FDIC has made progress toward implementing its systemic resolution authorities under the Dodd-Frank Act, but challenges remain. These challenges involve the FDIC fulfilling its insurance, supervisory, receivership management, and resolution responsibilities as it meets the requirements of the Dodd-Frank Act. These responsibilities are cross-cutting and require collaborative efforts among staff throughout the Corporation's headquarters and regional divisions and offices in implementing Titles I and II, including the Office of Complex Financial Institutions (OCFI), Division of Risk Management Supervision (RMS), Division of Resolutions and Receiverships (DRR), and Legal Division.

Of note with respect to the challenge of Dodd-Frank Act responsibilities, in April 2016, the FDIC and the Federal Reserve Board (FRB) announced a significant step forward in the use of the "living will" authority to require systemically important financial institutions to demonstrate they can fail in an orderly way at no cost to taxpayers. Specifically, following eight firms' submission of their living wills or resolution plans in July 2015, the FDIC and the Federal Reserve announced findings based on their review of the plans and conveyed required actions that firms needed to take for remediation. For five firms, the agencies jointly determined that the plans were not credible or would not facilitate an orderly resolution under bankruptcy. The FDIC and FRB jointly identified a number of deficiencies in those plans, as required by statute. Those five firms were required to remedy the deficiencies by October 1, 2016. If not, the firms could be subject to more stringent capital, leverage, or liquidity requirements, or restrictions on growth, activities, or operations. On December 13, 2016, the FDIC and the FRB announced that four of the five firms had adequately remediated deficiencies in their 2015 plans.

For two other firms, the FDIC and the FRB did not make a joint determination, but did find separately that in the two cases, the plans were not credible and would not facilitate an orderly resolution under bankruptcy. For the eighth and final firm, the shortcomings did not rise to the level of the statutory standard for a joint determination of non-credibility. In addition to the October deadline for the five plans referenced above, all shortcomings in the plans must be addressed by July 1, 2017.

Those involved in Dodd-Frank Act activities will continue to evaluate the resolution plans submitted by the largest bank holding companies and other SIFIs under Title I, develop strategies for resolving SIFIs under Title II, work to promote cross-border coordination and cooperation for the orderly resolution of a global SIFI, and coordinate with the other regulators in developing policy to implement the provisions of the Act.

Also, the FDIC will need to ensure that staff have the needed knowledge and experience to continue

to carry out risk assessments to identify supervisory, resolution, and insurance pricing-related risks in all insured depository institutions with more than $10 billion in assets, including those for which the FDIC is not the primary federal regulator, in addition to systemically important bank holding companies and nonbank financial companies subject to Title I of the Dodd-Frank Act.

Maintaining Effective Supervision and Preserving Community Banking

The FDIC's supervision program promotes the safety and soundness of FDIC-supervised insured depository institutions. The FDIC is the primary federal regulator for 3,790 FDIC-insured, state-chartered institutions that are not members of the Board of Governors of the Federal Reserve System. As such, the FDIC is the lead federal regulator for the majority of community banks. In the case of "de novo" institutions, the FDIC needs to continue to emphasize that these new banks satisfactorily address statutory factors, including adequacy of capital, future earnings prospects, and the general character and fitness of bank management.

We have pointed out in our past work that a key lesson from the crisis is the need for earlier regulatory response when risks are building. Even now, for example, as they operate in a post-crisis environment, banks may be tempted to take additional risks, engage in imprudent concentrations, or loosen underwriting standards. Some banks are also introducing new products or lines of business or seeking new sources for non-interest income, all of which can lead to interest rate risk, credit risk, operational risk, and reputational risk. Such risks need to be managed and addressed early-on during the "good times" before a period of downturn. RMS has continued to reinforce the importance of forward-looking supervision to assess the potential impact of an institution's new and/or growing risks and ensure early mitigation when necessary.

FDIC examiners need to continue to identify problems; bring them to bank management's attention; follow up on problems; bring enforcement actions as needed; ban individuals from banking, as appropriate; and be alert to such risks as Bank Secrecy Act and anti-money-laundering issues. In doing so, the Corporation needs to execute its supervisory authority in a fair, consistent manner. With respect to important international concerns, the FDIC also needs to support development of sound global regulatory policy through participation on the Basel Committee on Bank Supervision and other related sub-groups.

In light of technological changes, increased use of technology service providers (TSP), new delivery channels, and cyber threats, we have pointed out in past work that the FDIC's IT examination program needs to be proactive and bankers and Boards of Directors need to ensure a strong control environment and sound risk management and governance practices in their institutions. Importantly, with respect to TSPs, one TSP can service hundreds or even thousands of financial institutions, so the impact of security incidents in one TSP can have devastating ripple effects on those institutions. Controls need to be designed not only to protect sensitive customer information at banks and TSPs, but also to guard against intrusions that can compromise the integrity and availability of operations, information and transaction processing systems, data, and business continuity. Given the complexities of the range of cyber threats, the FDIC needs to ensure its examination workforce has the needed expertise to effectively carry out its IT examination function.

An article in the FDIC's Winter 2015 issue of *Supervisory Insights* highlights a number of steps the Corporation has taken to increase industry awareness of cyber risks and to provide practical tools to help mitigate the risk of cyber attacks. Among those, the FDIC has urged institutions to avail themselves of existing resources to identify and mitigate cyber risks; developed the "Cyber Challenge" exercise for community banks to use in assessing their preparedness for a cyber-related incident; offered a cybersecurity awareness training program for FDIC-supervised institutions and FDIC supervision staff

and management in each of the FDIC's regional offices; continued participation on the Federal Financial Institutions Examination Council's (FFIEC) Cybersecurity Critical Infrastructure Working Group to determine how well banks manage cyber security and assess banks' preparedness to mitigate cyber risks; and assisted in updating the FFIEC's IT Examination Handbook and related guidance.

In the coming months, the Corporation needs to continue efforts, along with the other regulators, to address these and other emerging risks and use all available supervisory and legal authorities to ensure the continued safety and soundness of financial institutions and affiliated third-party entities. It also needs to ensure effective information-sharing about security incidents with regulatory parties and other federal groups established to combat cyber threats in an increasingly interconnected world.

The FDIC Chairman continues to emphasize that one of the FDIC's most important priorities is the future of community banks and the critical role they play in the financial system and the U.S. economy as a whole. Local communities and small businesses rely heavily on community banks for credit and other essential financial services. These banks foster economic growth and help to ensure that the financial resources of the local community are put to work on its behalf. Consolidations and other far-reaching changes in the U.S. financial sector in recent decades have made community banks a smaller part of the U.S. financial system. Still, over the last several years, they have made up a larger percentage of all FDIC-insured banks and thrifts than at any other time over the last three decades. Their share of total industry loans has also remained relatively constant over the past decade.

The FDIC has sought to identify and implement changes to improve the efficiency and effectiveness of the community bank risk management and compliance examination processes, while still maintaining supervisory standards. To ensure the continued strength of the community banks, the Corporation will also need to sustain initiatives such as ongoing research, technical assistance to the banks by way of training videos on key risk management and consumer compliance matters, continuous outreach and dialogue with community banking groups, and attention to strengthening minority depository institutions.

Maintaining a strong examination program, conducting forward-looking supervisory activities for both small and large banks, applying lessons learned, being attuned to harmful cyber threats in financial institutions and technology service providers, and preserving community banking will be critical to ensuring stability and continued confidence in the financial system going forward.

Carrying Out Current and Future Resolution and Receivership Responsibilities

One of the FDIC's most important roles is acting as the receiver or liquidating agent for failed FDIC-insured institutions. The FDIC's responsibilities include planning and efficiently handling the resolutions of failing FDIC-insured institutions and providing prompt, responsive, and efficient administration of failing and failed financial institutions in order to maintain confidence and stability in our financial system.

As part of the resolution process, the FDIC values a failing federally insured depository institution, markets it, solicits and accepts bids for the sale of the institution, considers the least costly resolution method, determines which bid to accept, and works with the acquiring institution through the closing process. The receivership process involves performing the closing function at the failed bank; liquidating any remaining assets; and distributing any proceeds to the FDIC, the bank customers, general creditors, and those with approved claims. The FDIC seeks to close out or pursue professional liability claims within 18 months of an insured institution's failure, which can prove challenging as well.

The FDIC places great emphasis on promptly marketing and selling the assets of failed institutions and terminating the receivership quickly. Although

the number of institution failures has fallen dramatically since the crisis, these activities still pose challenges to the Corporation. As of December 31, 2016, DRR was managing 378 active receiverships with assets in liquidation totaling about $3.3 billion.

In addition, through purchase and assumption agreements with acquiring institutions, the Corporation has entered into shared-loss agreements (SLA). Since loss sharing began during the most recent crisis in November 2008, the Corporation has resolved 304 failures with accompanying SLAs. Under these agreements, the FDIC agrees to absorb a portion of the loss—generally 80 to 95 percent—which may be experienced by the acquiring institution with regard to those assets, for a period of up to 10 years. The FDIC entered into 304 SLAs from November 2008 through September 30, 2013, with an initial asset base of $216.5 billion. As of December 31, 2016, FDIC recoveries totaled $5.2 billion, representing 15.2 percent of the $34.1 billion in FDIC SLA payments.

As another resolution strategy, the FDIC entered into 35 structured sales transactions involving 43,315 assets with a total unpaid principal balance of $26.2 billion. Under these arrangements, the FDIC receiverships retain a participation interest in future net positive cash flows derived from third-party management of these assets. As of December 31, 2016, the unpaid principal balance in 26 active arrangements was $1.5 billion. The Corporation will continue to evaluate termination offers from limited liability company (LLC) managing members in deciding whether to pursue dissolution of the LLCs if in the best economic interest of the receiverships.

As time passes and recovery from the crisis continues, these risk sharing agreements will continue to wind down and certain active receiverships will be terminated. Given the substantial dollar value and risks associated with the risk-sharing activities and other receivership operations, the FDIC needs to ensure continuous monitoring and effective oversight to protect the FDIC's financial interests. As an example, a large number of commercial SLAs have reached their 5-year mark, resulting in the end of FDIC loss-share coverage but not the end of the commercial SLAs, which last 8 years. The last 3 years of commercial SLA coverage is for recoveries only. Acquiring institutions may not pursue recoveries as vigorously as they should because they may only share in a relatively small percentage of recoveries. The FDIC needs to be sure that acquiring institutions identify and remit recoveries to the Corporation.

While conditions in the economy and financial system have improved since the peak of the financial crisis, bank failures continue to occur. The Corporation has reshaped its workforce and adjusted its budget and resources in line with the trend of far fewer failures. Notably, in the case of the FDIC's resolutions and receiverships workforce, authorized staffing decreased dramatically from a peak of 2,460 in 2010 to authorized staffing of 564 for 2016. As of December 31, 2016, DRR on-board staffing totaled 537. DRR will continue to substantially reduce its nonpermanent staff each year, based on declining workload.

These staff reductions bring with them a loss of specialized experience and expertise that could impact the success of future, large-scale resolution and receivership activities. As discussed in connection with Dodd-Frank Act responsibilities, for example, the Corporation must continue to review the resolution plans of large bank holding companies and designated nonbank holding companies to ensure their resolvability under the Bankruptcy Code, if necessary, and in cases where their failure would threaten financial stability, administer their orderly liquidation. Carrying out such activities could pose significant challenges to those remaining staff in DRR who could be called upon to lead critical resolution activities.

Ensuring the Continued Strength of the Deposit Insurance Fund

Insuring deposits remains at the heart of the FDIC's commitment to maintain stability and public confidence in the nation's financial system.

Continuing to replenish the Deposit Insurance Fund (DIF) in a post-crisis environment is a critical activity for the FDIC. To maintain sufficient DIF balances, the FDIC collects risk-based insurance premiums from insured institutions and invests deposit insurance funds. A broad goal for the FDIC is that institutions that pose the greatest risk to the DIF have deposit insurance rates that are commensurate with that risk.

The DIF balance had dropped below negative $20 billion during the worst time of the crisis. As of December 31, 2016, the DIF balance had risen to $83.2 billion. While the fund is considerably stronger than it has been, the FDIC must continue to monitor the emerging risks that can threaten fund solvency in the interest of continuing to provide and administer the insurance coverage that depositors have come to rely upon. This is true for insured depositors at small banks as well as for claims at large depository institutions.

In response to the Dodd-Frank Act and in the interest of protecting and insuring depositors, the Corporation has designed a long-term DIF management plan. This plan complements the Restoration Plan, which is designed to ensure that the DIF reserve ratio will reach 1.35 percent by September 30, 2020. As of September 30, 2016, the reserve ratio had reached 1.18 percent, the highest reserve ratio in 8 years.

In February 2011, the FDIC Board decided to reduce overall assessment rates when the reserve ratio reached 1.15 and the Board reaffirmed that position in April 2016. Now a large majority of banks will pay lower deposit insurance assessments. Assessment rates for approximately 93 percent of banks with less than $10 billion in assets declined. Regular quarterly assessments declined on average by about one-third for these smaller institutions.

Additionally, since the ratio has reached 1.15 percent, banks with $10 billion or more in assets began paying temporary surcharges to bring the reserve ratio up to statutory minimums. Even with the surcharges, about one-third of large banks still pay lower total assessments because of the reduction in regular assessment rates. The FDIC is taking a balanced approach to restoring the health of the DIF as it seeks to reduce the risk that it will need to raise rates unexpectedly to address a future crisis and to help ensure stable and predictable assessments across the board.

Given the volatility of the global markets and financial systems, new risks can emerge without warning and threaten the safety and soundness of U.S. financial institutions and the viability of the DIF. The FDIC must be prepared for such a possibility. In the face of such threats, the FDIC needs to continue to disseminate data and analysis on issues and risks affecting the financial services industry to bankers, supervisors, and the public.

As part of its efforts, the FDIC also needs to continue collaborating with others involved in helping to ensure financial stability and protect the DIF. One important means of doing so is through participation with other financial regulators on the Financial Stability Oversight Council, created under the Dodd-Frank Act. This Council was established to provide comprehensive monitoring of stability in the U.S. financial system by identifying and responding to emerging risks to U.S. financial stability and by promoting market discipline.

The FDIC will also be challenged to contribute to global financial stability by continuing its engagement with strategically important foreign jurisdictions and playing a leadership role in international organizations that support robust, effective deposit insurance systems, crisis management and resolution programs, and bank supervision practices around the globe.

Promoting Consumer Protections and Economic Inclusion

The FDIC carries out its consumer protection role by providing consumers with access to information about their rights and disclosures that are required by federal laws and regulations. Its Consumer Response Center serves an important function in this regard. Similarly,

initiatives like the FDIC's Money Smart and Youth Savings programs go a long way towards educating the public about important consumer and financial matters. Importantly, the FDIC also examines the banks for which it is the primary federal regulator to determine the institutions' compliance with laws and regulations governing consumer protection, fair lending, and community investment. These activities require effective examiner training and regular collaboration with other regulatory agencies.

The Dodd-Frank Act consolidated many of the consumer financial protection authorities previously shared by several federal agencies into the Consumer Financial Protection Bureau (CFPB) and granted the CFPB authority to conduct rulemaking, supervision, and enforcement with respect to federal consumer financial laws; handle consumer complaints and inquiries; promote financial education; research consumer behavior; and monitor financial markets for risks to consumers. The FDIC coordinates with the CFPB on consumer issues of mutual interest and to meet statutory requirements for consultation relating to rulemakings in mortgage lending and other types of consumer financial services and products. The FDIC will need to continue to assess the impact of such rulemakings on supervised institutions, communicate key changes to stakeholders, and train examination staff accordingly.

The FDIC continues to work with the Congress and others to ensure that the banking system remains sound and that the broader financial system is positioned to meet the credit needs of consumers and the economy, especially the needs of creditworthy households that may experience distress. One of the challenges articulated by the FDIC Chairman is to continue to develop and implement targeted strategies to expand access to mainstream financial institutions by populations that are disproportionately likely to be unbanked or underbanked.

The FDIC conducts national surveys of unbanked and underbanked households every 2 years, in conjunction with the Census Bureau, to inform those strategies. The most recent survey, for example, determined that the share of unbanked households in the U.S. dropped in 2015 to 7.0 percent, representing a significant decline from the 7.7 unbanked rate reported in 2013 and the 8.2 unbanked rate in 2011. The survey also revealed a growth pattern in consumer use of mobile and online banking. For the unbanked households, smart phones are often the primary means of managing their accounts. The FDIC is further exploring the economic inclusion potential of mobile financial services.

In addition, the FDIC's Advisory Committee on Economic Inclusion, composed of bankers, community and consumer organizations, and academics, will continue to explore ways of bringing the unbanked into the financial mainstream. The FDIC's Alliance for Economic Inclusion initiative seeks to collaborate with financial institutions; community organizations; local, state, and federal agencies; and other partners to form broad-based coalitions to bring unbanked and underbanked consumers and small businesses into the financial mainstream.

The FDIC will need to sustain ongoing efforts to carry out required compliance and community reinvestment examinations, coordinate with the other financial regulators and CFPB on regulatory matters involving financial products and services, and pursue and measure the success of economic inclusion initiatives to the benefit of the American public.

Implementing Workforce Changes and Budget Reductions

The Corporation continues to reassess its current and projected workload along with trends within the banking industry and the broader economy. Based on that review, the FDIC expects a continuation of steady improvements in the global economy, a small number of insured institution failures, gradual reductions in post-failure receivership management workload, and further reductions in the number of 3-, 4-, and 5-rated institutions. While the FDIC will continue to need some temporary and term

employees over the next several years to complete the residual workload from the financial crisis, industry trends continue to confirm that there will be a steadily decreasing need for nonpermanent employees over the next several years.

Given those circumstances, the FDIC Board of Directors approved a $2.16 billion FDIC Operating Budget for 2017, 2.4 percent lower than the 2016 budget. In conjunction with its approval of the 2017 budget, the Board also approved an authorized 2017 staffing level of 6,363 positions for 2017, a 2.6 percent decrease from 2016 and 32 percent lower than the peak in 2011. This was the seventh consecutive reduction in the FDIC's annual operating budget.

As conditions improve throughout the industry and the economy, the FDIC will continue its efforts to achieve the appropriate level of resources; at the same time, however, it needs to remain mindful of ever-present risks and other uncertainties in the economy that may prompt the need for additional resources and new skill sets and expertise that may be challenging to obtain. The need for these new skill sets comes at a time when the Corporation is focusing on succession management, in light of a substantial number of FDIC staff, many "baby boomers," who are retiring. In that regard, the FDIC is continuing to work toward integrated workforce development processes as it seeks to bring on the best people to meet its changing needs and priorities, and do so in a timely manner. In all of its hiring efforts, the Corporation needs to ensure fairness and integrity in its processes and hiring practices and decisions. Most recently, the Corporation has emphasized its Workforce Development Initiative as a means of fulfilling the FDIC's future leadership and workforce capability needs. It has also focused on addressing resource needs to address the many challenges in divisions such as OCFI, RMS, and DRR, as previously discussed.

With respect to leadership at the uppermost levels of the Corporation, it is important to note that a vacancy currently exists on the FDIC Board of Directors—Jeremiah Norton left the FDIC in June 2015 and his seat on the Board remains vacant. The current FDIC Chairman's term is set to expire in November 2017, which would leave another position vacant. The FDIC Board has experienced such vacancies in the past and the FDIC IG at the time strongly advocated filling those Board positions. Now, given the myriad financial and economic concerns, emerging risks, Dodd-Frank Act responsibilities, important priorities and challenges facing the FDIC, and the advent of a new Administration, strong and sustained senior leadership is even more essential.

The FDIC has long promoted diversity and inclusion initiatives in the workplace. Section 342 of the Dodd-Frank Act reiterates the importance of standards for assessing diversity policies and practices and developing procedures to ensure the fair inclusion and utilization of women and minorities in the FDIC's contractor workforce. The Dodd-Frank Act also points to the Office of Minority and Women Inclusion as being instrumental in diversity and inclusion initiatives within the FDIC working environment. This office needs to ensure that it has the proper staff, expertise, and organizational structure to successfully carry out its advisory responsibilities to ensure diversity and inclusion throughout the Corporation.

The FDIC needs to sustain its emphasis on fostering employee engagement and morale on the part of all staff in headquarters, regions, and field locations. It looks to the annual Federal Employee Viewpoint Survey to provide a candid assessment of employee views of the FDIC workplace. The Corporation's diversity and inclusion goals and initiatives, Workplace Excellence Program, and Workforce Development Initiative are positive steps that should continue to help create a workplace that promotes diversity and equal opportunity.

Finally, an organization's overall corporate culture is essential to its success and, in July/August 2016, prompted in part by earlier OIG work, the FDIC Board of Directors reaffirmed the Corporation's

Code of Conduct and the six core values that underlie it: integrity, competence, teamwork, effectiveness, accountability, and fairness. The Chairman emphasized that these values apply not only to internal conduct but also externally, as FDIC leadership and staff interact with bankers, consumers, and other members of the public. In further support of these values, the Board prohibits retaliation against an employee who raises concern about conduct that appears to violate laws, rules, or the FDIC's supervisory policy. In that connection, the Chairman also underscored the importance of whistleblower protection in a message to all FDIC staff on the occasion of the U.S. Senate passing Resolution 522 on July 7, 2016, designating July 30, 2016, National Whistleblower Appreciation Day. This Resolution acknowledges and commemorates the contributions of whistleblowers to combat waste, fraud, and violations of law. As noted by the Chairman, the Resolution encouraged executive federal agencies to inform employees and contractors about the legal rights to "blow the whistle" by honest and good faith reporting of misconduct, fraud, misdemeanors, or other crimes to the appropriate authorities.

Ensuring Effective Enterprise Risk Management Practices

Enterprise risk management is a critical aspect of governance at the FDIC. Notwithstanding a stronger economy and financial services industry, the FDIC's enterprise risk management framework and related activities need to be attuned to emerging risks, both internal and external to the FDIC, that can threaten key business processes and corporate success. As evidenced in the challenges discussed above, certain difficult issues may fall within the purview of a single division or office, while many others are cross-cutting within the FDIC, and still others involve coordination with the other financial regulators and other external parties.

The Corporation needs to maintain effective controls, mechanisms, and risk models that can address a wide range of concerns—from specific, everyday risks such as those posed by use of corporate purchase or travel cards and records management activities, for example, to the far broader concerns of the ramifications of an unwanted and harmful cyber attack or the failure of a large bank or systemically important financial institution.

In July 2016, the Office of Management and Budget updated Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control. This circular defines management's responsibility for enterprise risk management (ERM) and internal control. It emphasizes the need to coordinate risk management and strong and effective internal control into existing business activities as an integral part of governing and managing an agency. Notwithstanding existing corporate risk management resources and mechanisms in place, the Corporation would be well served to examine and adopt those principles and practices embodied in the circular that make sense for the FDIC and ensure they are institutionalized, as intended by the circular. Doing so can help ensure that the Corporation's risk management processes and systems identify challenges early on, bring them to the attention of corporate leadership, and develop solutions. Given the range, complexity, and importance of many of the Corporation's current endeavors—for example, the personal identification validation project, email and hard copy records management practices, data breach prevention measures, personnel security initiatives, and the like, such an approach could help ensure more effective project management and other controls and strengthen oversight of often costly investments and mission-critical activities.

The Corporation's stakeholders—including the Congress, American people, media, and others—expect effective governance, sound risk management practices, and vigilant regulatory oversight of the financial services industry. The Corporation needs to maintain the trust and confidence that it has instilled over the years. The FDIC Board of Directors, senior

management, and individuals at every working level throughout the FDIC need to acknowledge, understand, and take ownership of current and emerging risks to the FDIC mission and be prepared to take necessary steps to mitigate those risks as changes occur and challenging scenarios that can undermine the FDIC's short- and long-term success present themselves. A corporate culture marked by integrity, efficiency, and transparency is essential to that end.