

STG Group, Inc.
Form 10-K
March 30, 2016

UNITED STATES

SECURITIES AND EXCHANGE COMMISSION

WASHINGTON, DC 20549

FORM 10-K

(Mark One)

ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934

For the fiscal year ended December 31, 2015

or

TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934

For the transition period from to

Commission file number 000-10030

STG GROUP, INC.

(Exact Name of Registrant as Specified on Its Charter)

Edgar Filing: STG Group, Inc. - Form 10-K

Delaware

(State or Other Jurisdiction of Incorporation or Organization)

46-3134302

(I.R.S. Employer Identification No.)

11091 Sunset Hills Road, Suite 200

Reston, Virginia

(Address of Principal Executive Offices)

20190

(Zip Code)

Registrant's telephone number including area code **(703) 691-2480**

Securities registered under Section 12(b) of the Exchange Act:

Title of Class

Common Stock, \$0.0001 par value

Securities registered under Section 12(g) of the Exchange Act: None

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act.

Yes No

Indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or Section 15(d) of the Act.

Yes No

Indicate by check mark whether the registrant (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days.

Yes No

Edgar Filing: STG Group, Inc. - Form 10-K

Indicate by check mark whether the registrant has submitted electronically and posted on its corporate Web site, if any, every Interactive Data File required to be submitted and posted pursuant to Rule 405 of Regulation S-T (§232.405 of this chapter) during the preceding 12 months (or for such shorter period that the registrant was required to submit and post such files).

Yes No

Indicate by check mark if disclosure of delinquent filers pursuant to Item 405 of Regulation S-K (§ 229.405 of this chapter) is not contained herein, and will not be contained, to the best of registrant's knowledge, in definitive proxy or information statements incorporated by reference in Part III of this Form 10-K or any amendment to this Form 10-K.

Yes No

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, or a smaller reporting company. See definitions of "large accelerated filer," "accelerated filer," and "smaller reporting company" in Rule 12b-2 of the Exchange Act. (Check one):

Large accelerated filer Accelerated filer
Non-accelerated filer Smaller reporting company

(Do not check if smaller reporting company)

Indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act).

Yes No

The aggregate market value of the common stock held by non-affiliates of the registrant, computed by reference to the closing sales price for the registrant's common stock on June 30, 2015 (the last business day of the registrant's most recently completed second fiscal quarter), as reported on the NASDAQ Capital Market, was approximately \$72,450,000.00.

Edgar Filing: STG Group, Inc. - Form 10-K

The number of shares outstanding of the registrant's common stock as of March 21, 2016 was 16,107,071.

STG GROUP, INC.

Table of Contents

| | Page |
|--|-------------|
| PART I | |
| <u>Item 1. Business</u> | 3 |
| <u>Item 1A. Risk Factors</u> | 17 |
| <u>Item 1B. Unresolved Staff Comments</u> | 35 |
| <u>Item 2. Properties</u> | 35 |
| <u>Item 3. Legal Proceedings</u> | 36 |
| <u>Item 4. Mine Safety Disclosures</u> | 36 |
| PART II | |
| <u>Item 5. Market for Registrant’s Common Equity, Related Stockholder Matters, and Issuer Purchases of Equity Securities</u> | 36 |
| <u>Item 6. Selected Financial Data</u> | 38 |
| <u>Item 7. Management’s Discussion and Analysis of Financial Condition and Results of Operations</u> | 39 |
| <u>Item 7A. Quantitative and Qualitative Disclosure About Market Risk</u> | 61 |
| <u>Item 8. Financial Statements and Supplementary Data</u> | |
| <u>Item 9. Changes in and Disagreements with Accountants on Accounting and Financial Disclosures</u> | 94 |
| <u>Item 9A. Controls and Procedures</u> | 94 |
| <u>Item 9B. Other Information</u> | 96 |
| PART III | |
| <u>Item 10. Directors, Executive Officers and Corporate Governance</u> | |

Item 11. *Executive Compensation*

Item 12. *Security Ownership of Certain Beneficial Owners and Management and Related Stockholder Matters*

Item 13. *Certain Relationships and Related Transactions, and Director Independence*

Item 14. *Principal Accounting Fees and Services*

PART IV

Item 15. Exhibits, Financial Statement Schedules 96

SIGNATURES 99

EXHIBIT INDEX 101

PART I

INTRODUCTORY STATEMENT

The information contained in this report pertains to the registrant, STG Group, Inc. References in this annual report to “STGG,” the “Company,” “we,” “our” and “us” refer to STG Group, Inc. and its subsidiaries.

CAUTIONARY NOTE REGARDING FORWARD-LOOKING STATEMENTS

We make forward-looking statements in this Annual Report on Form 10-K. These forward-looking statements relate to outlooks or expectations for earnings, revenues, expenses or other future financial or business performance, strategies or expectations, or the impact of legal or regulatory matters on business, results of operations or financial condition. Specifically, forward-looking statements may include statements relating to:

- the future financial performance of the Company;
- expansion plans and opportunities;
- maintaining/increasing our growth rates through marketing and an effective sales force;
- maintaining our technology platforms and continuing to develop enhancements;
- maintaining cost-effectiveness of technology and operations;
- maintaining and successfully bidding for government contracts;
- changes in economic, business, competitive, technological and/or regulatory factors;
- identify and consummating acquisitions on an accretive basis; and

other statements preceded by, followed by or that include the words “estimate,” “plan,” “project,” “forecast,” “intend,” “expect,” “anticipate,” “believe,” “seek,” “target” or similar expressions.

Should one or more of these risks or uncertainties materialize, or should any of the underlying assumptions prove incorrect, actual results may vary in material respects from those expressed or implied by these forward-looking statements. You should not place undue reliance on these forward-looking statements. These forward-looking statements are based on information available to us as of the date of this Annual Report on Form 10-K and current expectations, forecasts and assumptions and involve a number of risks and uncertainties. Accordingly, forward-looking statements should not be relied upon as representing our views as of any subsequent date and we do not undertake any obligation to update forward-looking statements to reflect events or circumstances after the date they were made. These forward-looking statements involve a number of known and unknown risks and uncertainties or other assumptions that may cause actual results or performance to be materially different from those expressed or implied by these forward-looking statements. Some factors that could cause actual results to differ include:

- success in retaining or recruiting, or changes required in, officers, key employees or directors;
- economic weakness, either nationally, or in the local markets in which we operate;
- the size of our addressable markets and the amount of U.S. government spending on private contractors;
- adverse litigation or arbitration results;

the potential liquidity and trading of our securities;

risks and costs associated with regulation of corporate governance and disclosure standards (including pursuant to Section 404 of the Sarbanes-Oxley Act);

the risk factors listed in this Annual Report on Form 10-K under “*Risk Factors*” beginning on page 17.

changes in economic, business, competitive, technological and/or regulatory factors; and,

competitors in our various markets.

ITEM 1 BUSINESS

Description of Transaction

The Company (formerly known as Global Defense & National Security Systems, Inc.), a former special purpose acquisition company focused on the U.S. defense and national security sector, successfully completed after the close of business November 23, 2015 (the “Closing Date”) the business combination (the “Business Combination”) with STG Group, Inc. (“STG Group” or the “Predecessor”), a provider of cyber, software and intelligence solutions to the U.S. government. At the closing of the Business Combination, the Company changed its name to “STG Group, Inc.” The Business Combination was consummated pursuant to the stock purchase agreement (the “Business Combination Agreement”), dated as of June 8, 2015, by and among the Company, the Predecessor, the stockholders of the Predecessor, Global Defense & National Security Holdings LLC (the “Sponsor”) and Simon S. Lee, as Stockholders’ Representative.

In connection with the closing of the Business Combination, the Predecessor changed its name to “STG Group Holdings, Inc.” (“STG Group Holdings”). Unless the context otherwise requires, the “Company”, “we,” “us,” and “our” refers STG Group, Inc.

Pursuant to the Business Combination Agreement, upon the effectiveness of the Business Combination shares of common stock of STG Group were exchanged for cash and validly issued shares of Company Common Stock paid and issued to the Predecessor’s stockholders. The Business Combination purchase price of \$170.9 million was subject

to working capital and other customary adjustments determined at the closing of the Business Combination in accordance with the terms of the Business Combination Agreement. The Business Combination occurred on November 23, 2015, and the consideration paid to the Predecessor's stockholders for their shares of STG Group common stock was \$177.0 million, consisting of \$68 million in cash (the "Cash Consideration"), \$7 million in conversion shares (658,513 shares) ("Conversion Shares") and \$90.5 million in common equity, or 8,578,199 shares, valued at approximately \$10.55 per share, issued by the Company, and \$6.8 million of purchase price adjustments for cash on the balance sheet and net working capital differences between the estimated working capital at close and the targeted working capital of \$10.1 million. The Company issued to the Predecessor's stockholders 445,161 shares (\$4.7 million) of Company Common Stock held by the Sponsor that was contributed by the Sponsor to the Company immediately prior to the closing of the transactions contemplated by the Business Combination Agreement.

In addition, at close, the Sponsor transferred to the Predecessor's stockholders 35,000 shares of Company common stock immediately prior to closing the transaction.

If, immediately following the closing of the transaction, the share consideration was, in the aggregate, less than 56.7% of the outstanding shares of Company Common Stock, as of the closing, a portion of the Cash Consideration may have been exchanged for additional shares of Company Common Stock at a price of \$10.55 per share, so that the Predecessor's stockholders would own, in the aggregate, 56.7% of the outstanding shares of Company Common Stock following the closing of the Business Combination. In addition, in the event that the transaction otherwise did not qualify for the tax treatment described in the Business Combination Agreement, a portion of the Cash Consideration would have been exchanged for additional shares of Company Common Stock at a price of \$10.55 per share, so that the Predecessor's stockholders, the Sponsor and any other person who received shares of Company Common Stock in connection with an equity financing completed in connection with the closing, would own 80% of the outstanding shares of Company Common Stock at closing. The Cash Consideration was increased by \$5.9 million by the amount of estimated working capital and cash at close exceeding the defined threshold.

The Cash Consideration was paid using proceeds held in our Trust Account and the balance of the Cash Consideration was paid using proceeds from debt financing. The remainder of the proceeds from the debt financing was used by the Company to pay debt and transaction related expenses and for general corporate purposes after closing. The Company finalized debt financing of \$81.75 million at close, while remaining cash raised in the Company's IPO and remaining in trust in the amount of \$8.3 million was transferred from the Trust (as defined below) to the Company at close. Shares redeemed at close amounted to 2,031,383 at \$10.63 per share (\$21.6 million).

On November 23, 2015, the Company entered into a Second Amended and Restated Backstop Common Stock Purchase Agreement (the "Backstop Purchase Agreement") with the Sponsor. The Backstop Purchase Agreement granted the Sponsor the right to purchase shares of Company Common Stock, at a price of \$10.63 per share (the "Backstop Purchase"). The purchase right was exercisable only in the event, and to the extent, that the Company did not meet the Threshold Cash Amount. The term "Threshold Cash Amount" means \$20,000,000 in cash available to the Company from (1) the Trust Account at the closing of the Business Combination following the payment in full to Public Stockholders who have requested to be redeemed in connection with the closing of the Business Combination, and (2) the payment of any aggregate purchase price for the Backstop Purchase. In connection with the closing of the Business Combination, the Sponsor purchased 1,030,103 shares for consideration of approximately \$10.95 million.

The Company declared a dividend of one share of Company Common Stock for every 1.06 shares of Company Common Stock payable to stockholders of record immediately following the consummation of the Business Combination, which occurred on November 23, 2015. The Sponsor, with respect to the shares of Company Common Stock held by the Sponsor and any shares that would have been able to have been acquired by the Sponsor upon any conversion of the convertible promissory notes held by the Sponsor prior to the Closing, and the Predecessor's stockholders, agreed to forfeit any Dividend Shares they would have been entitled to in exchange for no consideration. The Sponsor did not forfeit any right to receive any Dividend Shares in respect of any shares it acquired pursuant to the Backstop Purchase and the Predecessor's stockholders did not forfeit any right to receive Dividend Shares with respect to the Conversion Shares. Payment of the dividend was contingent upon the closing of the Business Combination and made on November 30, 2015, as soon as practicable after close of the Business Combination.

On July 17, 2015, the Company held a special meeting of stockholders (the "July Extension Meeting"). At the July Extension Meeting, the stockholders approved amendments to the Charter to extend the date by which the Company was to consummate its initial business combination from July 24, 2015 to October 24, 2015. In accordance with our amended and restated certificate of incorporation ("Charter"), in connection with the July Extension Meeting and the approval of the amendments to the Charter, our public stockholders were entitled to redeem their Company Common Stock for cash equal to their pro rata share of the aggregate amount then on deposit in the Trust Account, including any amounts representing interest earned on the Trust Account, less any interest released to the Company to pay franchise or income taxes. Our stockholders redeemed 876,072 shares of Company Common Stock at a price of \$10.55 per share, for a total redemption of approximately \$9,242,560 that was effected on July 24, 2015.

In addition, in connection with the July Extension Meeting, on July 21, 2015, the Company issued a non-interest bearing promissory note to the Sponsor for an aggregate of approximately \$361,436. The Company used the proceeds from the note to deposit \$0.06 per share that was not redeemed in the Trust Account. In connection with the October Extension Meeting, on October 23, 2015, the Company issued a non-interest bearing promissory note to the Sponsor for an aggregate approximately \$56,300. The Company used the proceeds from the note to deposit \$0.02 per share that was not redeemed in the Trust Account. The notes were repaid immediately following consummation of our initial business combination. After giving effect to the redemptions and the additional deposits, there was approximately \$29,921,377 in the Trust Account as of October 30, 2015, or approximately \$10.63 per public share. There were 3,209,123 shares redeemed at \$10.61 per share.

In connection with the closing, the Company's public stockholders elected to redeem 2,031,383 shares of Common Stock pursuant to the terms of the Company's amended and restated certificate of incorporation, at a price per share of \$10.63, resulting in a total payment to redeeming stockholders of \$21,593,601.29. See also "**Management's Discussion and Analysis Goodwill, Other Intangible Assets and Other Long-Lived Assets**"

OUR BUSINESS

We provide specialist cyber, software and intelligence solutions to U.S. government organizations with a national security mandate. Our solutions are integral to national security-related programs run by more than 50 U.S. government agencies, including the Department of Defense, the Intelligence Community, the Department of Homeland Security, the Department of State and other government departments with national security responsibilities. Our programs are predominantly funded from base budgets and are essential to the effective day-to-day operations of our customers.

Our operational strength and track record has been established in securing highly sensitive, mission-critical national security networks, solving complex technology problems in mission-critical contexts and providing decision makers with actionable intelligence from multiple data sources.

Our primary areas of expertise include:

- ◆ Security information and event management
- ◆ Network intrusion detection and prevention
- ◆ Application vulnerability assessment
- ◆ Agile software development
- ◆ Command and control system development
- ◆ Complex application development
- ◆ Advanced collection and analysis
- ◆ Multi-intelligence exploitation and dissemination

Multi-lingual intelligence analysis

We are SEI CMMI Maturity Level 3 Rated and hold certifications in ISO 9001:2008 and ISO/IEC 20000-1:2011. We fully integrate ISO 20000-1:2011 quality aspects into our corporate engineering methodology to ensure we deliver high-quality products and services on time and within budget.

We employ over 850 cybersecurity, software development and intelligence analysis professionals who deliver these solutions in both the continental United States and in approximately 6 overseas locations.

We have generated more than \$190 million in annual revenue since 2009.

Our revenue for 2015 was \$193.6 million and our revenue for 2014 was \$209.7 million. As of December 31, 2015, our total backlog was \$253 million, of which \$107 million was funded and \$146 million was unfunded. For a discussion of how we calculate backlog, see “— *Backlog*”.

The Predecessor was founded in 1986 as the Software Technology Group. Over that time, we have built strong, trusted and enduring relationships with a wide range of Federal Government customers, supporting their mission-critical operations across a very broad contract base. We have achieved an average period of continuous performance of more than a decade, and sustain a relatively low degree of contract concentration — in 2015, our largest single contract award represented just **17%** of total revenues; the top 5 contracts represented **47%** of total revenues.

We are currently contracted with 50 U.S. Federal Government organizations, and we derive the majority of our revenue from contracts with U.S. Government agencies with a national security mission. For 2015, we derived approximately 43% of our revenue from the Department of Defense; approximately 32% from the Department of State; approximately 20% from other Federal Civilian agencies, with most of that revenue coming from the Department of Homeland Security; and approximately 5% coming from the Intelligence Community.

Our Capabilities

The Company specializes in three core areas of capability:

Cyber Security and Secure Information Systems — securing highly sensitive, mission-critical national security networks

- **Software Development, Systems and Services** — solving complex problems in mission-critical contexts

Intelligence and Analytics — gathering and analyzing data from multiple sources to provide high quality, actionable intelligence across multiple contexts

Cybersecurity and Secure Information Systems

Our mission is to establish, develop and sustain secure, resilient, mission-critical information systems. We deliver across the cybersecurity spectrum with secure network engineering, information assurance platform deployment and incident response capabilities. In addition, we architect network configuration for optimal performance.

Our technical experts develop and integrate technologies to perform a range of essential tasks, from situational awareness and vulnerability assessments to encryption and authentication, each with the aim of supporting the protection of enterprise networks critical to the national interest.

We provide contextual technical analysis to enhance client understanding of the threats they face, and remain technology-neutral to provide the right tools to meet mission objectives.

The solutions we offer our customers in this area include:

Security Information & Event Management. We provide customers with an integrated, holistic view of their organization's network activity, identifying and prioritizing the handling of anomalous events across the entire spectrum of users and devices.

Network Intrusion Detection & Protection. We design and implement systems that gather and analyze network data in order to identify internal and external cybersecurity breaches.

Identity & Access Management. We create systems that facilitate the oversight and management of digital identities — controlling access rights to resources and information across complex networks.

Network Vulnerability Assessment. We implement and oversee systems that continuously scan and test networks to identify potential vulnerabilities, assess the risk associated those vulnerabilities and address risk mitigation.

Software Development, Systems and Services

Our mission is to create technology solutions tailored to our customers' needs. Our agile software development practices, ranging from iterative system builds to highly integrated enterprise platforms, scale dynamically to system demands.

Our systems and software engineering approach is highly adaptable to complex mission demands, ranging from multi-stakeholder identity and big data reconciliation to integrated mobile applications processing geospatially-based information.

We work to align and incorporate legacy enterprise systems, which are leveraged with our software methods and advanced technologies to deliver greatly enhanced functional value.

The solutions we offer our customers in this area include:

Agile Software Development. We deliver software development services with an emphasis on providing functionality and flexibility on complex IT programs, incorporating legacy system sustainment and migration and new application development.

Command & Control Systems Development. We develop software and systems that deliver a common operating picture for decision makers to help them evaluate, plan, direct and coordinate resources and operations.

Complex Application Development. We design customized software solutions that help integrate information drawn from disparate sources and automate highly complex business processes.

Decision Support Systems (DSS) Integration. We develop software applications and systems that combine raw data, structured models and analytic techniques to better enable our customers to make decisions in highly complex and changing circumstances.

Database Design & Development. We design and integrate structured data models across various legacy and new applications and databases to improve the value and utility of customer data and the quality of operational decision-making.

Intelligence and Analytics

Our mission is to provide our customers with high quality intelligence as the basis for critical decision-making. We work to a proven, rigorous methodology that combines specialized analysts with leading technologies.

Our experts gather data from multiple sources, analyze and fuse the data to provide clarity and situational context, and disseminate the resulting intelligence to a diverse range of stakeholders. The Company employs a combination of large-scale processing and qualitative analysis to produce high quality intelligence products.

Our approach supports strategic and tactical decisions in the fields of defense and intelligence, homeland security, and diplomatic affairs.

The solutions we offer our customers in this area include:

Advanced Collection & Analysis Tools. We design and employ leading-edge technology solutions that enhance the collection and analysis of high volumes of all-source data to deliver high quality, actionable intelligence to decision makers.

Multi-Intelligence Exploitation. We create integrated solutions combining technology with our strong analytic expertise to gather, filter, fuse and visualize data from a wide variety of signals and sources.

Intelligence Analysis Training. We provide comprehensive tradecraft training covering the full intelligence cycle, including advanced data harvesting and analysis tools, social media analysis, analytic visualization techniques and sustaining a network of highly specialized professionals, such as intelligence analysts, linguists and cultural advisors.

Multi-Lingual Intelligence Analysis. We provide intelligence collection and analysis across 46 different languages through highly specialized, cleared professionals, including intelligence analysts, linguist and cultural advisors with a deep understanding of the political, social, cultural and economic contexts at source.

Our Market Opportunity

U.S. government defense and national security spending, incorporating multiple federal agencies and departments, is driven by a complex range of persistent and evolving threats to the U.S. homeland and to its interests overseas. Over

the last decade, the U.S. government has realigned the strategic priorities of the U.S. national security community, its capabilities and posture to achieve a sustainable balance between the ability to face down conventional threats from opposing states, the ability to combat non-state actors or asymmetric threats, and the ability to defeat threats from new technologies. These efforts have been concentrated on counter-terrorism, stabilizing fragile regions of strategic importance to the U.S., and counterinsurgency. Most recently and as emphasized in the 2014 Quadrennial Defense Review (QDR), these efforts have also addressed contemporary threats and challenges such as those related to information and cybersecurity and the associated threats to critical national infrastructure.

In each case, emphasis has been given to developing new technologically-driven capabilities to strengthen operational decision making through improved information and intelligence, deliver precision in offensive operations in complex environments, and strengthen both defensive and offensive capabilities in the cyber domain.

In the March 2013 Worldwide Threat Assessment report to the Senate Select Committee on Intelligence, the Director of National Intelligence, James R. Clapper, listed the cyber threat as the number one strategic threat to the United States, placing it ahead of terrorism for the first time since the attacks of September 11, 2001. Since then, the cyber threat has remained the number one strategic threat to the United States, as reported in the February 2015 Worldwide Threat Assessment. Over the past few years the number of cyber-attacks perpetrated by criminals, hackers and foreign nations against the U.S. Government's networks has risen sharply. Potential state and non-state adversaries conduct malicious cyber activities against U.S. interests globally and in a manner intended to test the limits of what the U.S. and the international community will tolerate. Actors may penetrate U.S. networks and systems for a variety of reasons, such as to steal intellectual property, disrupt an organization's operations for activist purposes, or to conduct disruptive and destructive attacks to achieve military objectives.

Since developing its first cyber strategy in 2011, the Department of Defense (DoD) has made significant investment and progress in building its cyber capabilities, developing its organizations and plans, and fostering the partnerships necessary to defend the country and its interests. However, as potential adversaries have also invested significantly in advancing their cyber capabilities, additional investment by the DoD will be needed to counter potential cyberattacks against the United States. As outlined in the 2014 Quadrennial Defense Review, the DoD has stated it will continue to invest in improving and expanding its cyber capabilities and forces to enhance the department's ability to conduct cyberspace operations, support military operations worldwide, and ensure U.S. national security.

U.S. national security is entrusted to a wide range of government organizations, including the Department of Defense, Department of State (DoS), Department of Homeland Security (DHS), and the Intelligence Community (IC). The FY 2016 President's DoD budget request accounts for approximately 14.7% of the total budget authority requested by the current Administration. The FY 2016 DoD budget request is \$585.3 billion, including a base budget of \$534.3 billion and \$50.9 billion for overseas contingency operations, representing an increase in the DoD base budget of \$38.2 billion from the 2015 enacted DoD base budget of \$496.1 billion. The DoD projects the base budget will increase to \$570.0 billion by 2020.

The FY 2016 President's DoS and United States Agency for International Development (USAID) budget request is \$50.3 billion, including a base budget of \$43.2 billion and \$7.0 billion for overseas contingency operations, representing an overall budget increase of approximately \$2.8 billion from the FY 2015 estimated budget of \$47.5 billion. The FY 2016 budget allocation for the IT Central Fund (ITCF) is \$234.4 million, an 8.1% increase over the FY 2015 estimated budget of \$216.8 million. The ITCF modernizes critical IT systems and maintains essential IT services throughout the department.

The FY 2016 President's DHS budget request is \$41.2 billion, compared to \$38.2 billion in FY 2015. As DHS has stated that safeguarding and securing cyberspace is a key focus area for the department, the FY 2016 budget request supports the DHS's two primary cyber acquisition programs: \$497.8 million for Network Security Deployment, which enables the department to detect malicious traffic targeting federal networks and prevent malicious traffic from harming those networks, and \$102.6 million for the Continuous Diagnostics and Mitigation (CDM) program, which provides hardware, software, and services designed to support activities that strengthen the operational security of federal networks.

U.S. national security activities are also conducted by the U.S. Intelligence Community, a group composed of 17 agencies, departments, organizations, and branches of the U.S. military, which are organized to gather, analyze, and distribute intelligence. For FY 2016, the collective base budget request of the IC included \$17.9 billion for the Military Intelligence Program (MIP) and \$53.9 billion for the National Intelligence Program (NIP). The FY 2016 budget allocations represent growth of 7.8% and 6.9% over the FY 2015 budget estimates for the MIP of \$16.6 billion and NIP of \$50.4 billion, respectively. Key NIP initiatives include improving integration of programs spread across the 17 IC elements, expanding the use of shared IT capabilities, continuing to support the protection and security of the critical networks that facilitate IC information-sharing, and ensuring that mission-critical intelligence information flows anywhere and anytime it is required.

Below is an outline of the key areas of capability that we believe the U.S. government will continue to prioritize as critical to its defense and national security strategies and that we believe will drive continued growth in our target markets.

IT Systems and Support Spending

The operations of U.S. defense and federal agencies and the national security community demand a wide variety of technology-based systems and information that are increasingly integrated with support services and solutions in order to successfully offer a range of capabilities that support specific essential missions. These areas include, but are not limited to, C4ISR (command, control, communications, computers, intelligence, surveillance, and reconnaissance), information technology and related services, and other key support services.

Military operations and the modern warfighter rely on integrated technology platforms comprised of C4ISR systems and related information technology architectures (Mission IT). These platforms link networks of signals and sensors to people and platforms, providing greater interoperability within and between allied defense forces, enabling intelligent decision making, and delivering more operationally and cost-effective solutions to the defense and national security communities. In addition, the continuous reliance on C4ISR systems and Mission IT demands the frequent maintenance and upgrade of the platforms. The federal government procures systems and software engineering, integration, and technology development services to ensure that the technology is able to perform effectively, address evolving and complex challenges, and be customized for specific missions.

Information technology in the federal government spans a variety of initiatives in addition to areas focused on mission-oriented defense and national security, such as the growth and management of the significant administrative IT backbone of the defense and intelligence communities, which enables more routine but necessary communication. In addition, there is a complex systems architecture for managing the health and welfare of personnel. Furthermore, technology advancements have enabled new capabilities in information sharing which DoD and federal agencies are seeking. These agencies are focused on expanding, upgrading, and integrating their IT architecture to enhance information security, facilitate information sharing, increase efficiency, and mitigate costs.

Critical to supporting a wide range of government organizations, including the DoD, DHS, DoS and the Intelligence Community, in their national security initiatives, are the products and services related to information technology. According to the Federal Chief Information Officer, the total federal IT budget request for FY 2016 is approximately \$86.4 billion, including the DoD IT budget request of \$37.3 billion, representing an increase of 2.9% from the FY 2015 DoD IT budget request of \$36.3 billion.

Due to an emphasis on cost effective federal IT spending, agencies have increased their use of agile development practices and evidence in the IT portfolio illustrates that agile projects have been nearly twice as likely to deliver on time as those using traditional development techniques, and have been 40% more likely to deliver planned capabilities on budget. The DoS, a leader in adopting agile development, has improved its average project delivery time from 235 days in May 2013 to 111 days.

Cybersecurity and Secure Information Systems

Cyber attacks target networks and attempt to disrupt or sabotage information and control systems. Cyber attacks targeting networks to access sensitive data, disrupt systems and operations, and sabotage critical infrastructure are increasing in both frequency and sophistication, with perpetrators able to operate individually or in organized cells from anywhere in the world as part of terrorist, criminal or state networks. In recognition of these dynamics and the threats they pose to U.S. national security, the U.S. government is channeling greater resources into the drive to identify the sources of such attacks and develop and implement effective counter-measures. Although this drive is not simply a matter of technology, we believe that the development of advanced technological responses will remain the key element of defending networks, systems and critical infrastructure. In April 2015, the DoD outlined a new comprehensive cyber strategy with the purpose of guiding the development of DoD's cyber forces and strengthening its cyber defense and cyber deterrence posture. The DoD's cyber strategy focuses on building cyber capabilities and organizations for three principal cyber missions: (1) defend DoD networks, systems and information; (2) defend the U.S. and its interests against cyber attacks of significant consequence; and (3) provide integrated cyber capabilities to support military operations and contingency plans.

In FY 2016, the President's budget proposes approximately \$14 billion in cybersecurity funding to enhance America's cyber capabilities. The budget continues to support the construction of the Joint Operations Center of U.S. Cyber Command (USCYBERCOM) at Fort Meade, Maryland, which is scheduled for occupation in FY 2018. The DoD's budget also includes \$12.3 billion in science and technology investment to advance U.S. technological superiority, a portion of which supports cyberspace programs and other research and technology projects to develop the requisite tools to accomplish the mission to protect national interests.

Competitive Strengths

Agile Technology Development Tailored to Customer Needs

Our innovative approach to technology development gives us the ability to adapt quickly to customer needs in a rapidly evolving technology environment. Many larger prime contractors can have difficulty incorporating newer, disruptive technologies because their business models rely on larger programs of record and multi-year technology development cycles to support larger overhead. Our approach enables us to create and deploy the most effective and cost-effective solution. In a changing procurement climate, this type of creativity and agility is critical. In addition to being more innovative and adaptive than many larger players, we believe we are also more stable and established than many small businesses in the Defense Technology market. Customers require financial and operational stability, especially in mission-critical contexts, and we have an established, trusted record of high-level performance that spans four decades. Additionally, many smaller businesses do not have the talent or the infrastructure to support programs that require world-class capabilities to protect national security interests.

Established, Long-Standing Customer Relationships

The Company has developed trusted, enduring relationships across an exceptionally broad customer base in the defense, national security and federal/civilian landscape, which is a testament to our customers' sustained confidence in our capabilities and our commitment to exceptional delivery. Our average period of continuous performance across our customer base is over a decade. We have worked with the U.S. Army for 17 years, the Department of State continuously for more than 20 years, the Department of Defense for over 17 years, the Department of the Treasury for over 15 years, and key elements of the Intelligence Community for over 12 years.

Diverse Contract Base

In addition to a diverse customer base, the Company is positioned on a wide range of contract vehicles, atypically broad for a company our size. We have positions on NETCENTS II, ITES-2, EAGLE II, CIO-SP3, SPAWAR ICO, GSA Alliant, and another large classified ID/IQ, as well as numerous single awards. Our breadth and diversity of contract vehicles provides our customers with various options to procure the solutions they require.

Strong Backlog and New Business Pipeline

We had backlog of \$253 million on active contracts as of December 31, 2015, of which \$107 million was funded and \$146 million was unfunded, spanning more than **57** discrete contracts or task orders. Because we perform tasks that are essential to the day-to-day operations and core missions of our customers, the budgets for our business are well protected and growing. Additionally, we have a current pipeline of almost \$3.2 billion of potential new business opportunities that we are currently pursuing or prospecting.

Experienced and Proven Leadership Team and Highly Skilled Workforce

The Company's directors and officers have combined experience spanning many years of acquiring, leading and growing operating companies addressing US national security priorities, and working at senior levels in the US government's defense and national security communities. Our workforce is staffed by highly skilled, qualified professionals, 84% of which have security clearances, with over 44% holding clearances to Top Secret and above. Over many years, the workforce has consistently earned the trust and confidence of key elements of the U.S. government's national security community responsible for handling much of the nation's most sensitive and mission-critical information.

Our Growth Strategy

Having established a strong platform in the mid-tier market, our objective is to consolidate, grow, and re-position the business as a technology innovator and provider of advanced solutions in the area of cybersecurity, agile software development, and integrated intelligence and data analytics in order to realize a premium valuation as the leading agile and sustainable mid-tier market player. Achieving this objective requires a detailed strategy to drive stronger organic growth in higher margin, high-growth market areas, and accelerated growth through strategic acquisitions using our proprietary mergers and acquisitions pipeline.

Organic Growth

We believe that the Company is well positioned to achieve strong platform growth, combining our significant, differentiated capabilities with our extensive network of government and industry relationships and experience of managing continuous operating improvements to enhance profitability and customer performance. The Company expects to achieve stronger organic growth through deeper and broader client relationships, a sustained emphasis on business efficiencies and the accelerated development of new solutions and capabilities.

Key areas of organic improvement to realize this growth include:

Business Development

The Company completed a detailed review of the business development strategy and its associated pipeline, people, processes and tools. As a result, the following areas of customer requirement have been prioritized for opportunity capture, each with significant alignment to current programs and capabilities; Software Development, Modernization and Enhancement (DME), Cyber Protection and Computer Network Defense (CND), and medium to large IT support services.

In addition, the Company has achieved greater alignment between its business development processes and human capital to allow for a more focused and effective application of resources against these identified opportunities. Business Development personnel have been centralized under a single reporting line with direct oversight by the Chief Integration Officer. Several key leadership roles have been filled to include a new Vice President of Business Development and a new Director of Proposal Operations. Our growing pipeline of opportunities has highlighted the need for additional resources to ensure effective capture management. Recruitment is underway for suitably qualified

senior business development specialists. Finally, the capture management process itself has been re-invigorated with focused opportunity reviews conducted by senior management to ensure full alignment of effort and seamless functional support across the business.

Optimize Operational Efficiency

Immediately following the Business Combination, the Company completed a reorganization of its operations into the three competency-based Sectors – Cyber Security and Secure Information Systems (CSIS); Software Development Systems and Services (SDDS), and Intelligence and Analytics (IA). This organizational realignment has allowed us to deliver our solutions more efficiently across all the markets we serve and reduce cost in overhead and G&A. With these changes, we created an operating model that is expected to improve margins and increase the opportunities for our senior management team to be more connected with our customers to deepen relationships and drive cross selling opportunities.

The Company is also in the process of completing the integration of its Quality Management System (QMS). Within the next three months, we expect to completely integrate our ISO 9001, ISO 20000, and ISO 27001 certifications under a single quality system. We believe this will help to ensure our continued ability to meet fully both the rigorous service delivery requirements of our customers and the stringent operating standards of a public company. The training program associated with the roll-out of the new system is designed to ensure that every Company employee is equipped with the knowledge and tools to operate to a consistent set of proven operational, financial, and human resources processes and procedures.

Significant Cross-Selling Opportunities

Significant opportunities exist for the Company's differentiated capabilities to be marketed and sold across adjacent clients in the defense, federal civilian, and intelligence communities. The creation of the Cyber Security and Secure Information Systems (CSIS), Software Development Systems and Services (SDSS) and Intelligence and Analytics (IA) Sectors has allowed for a much more effective segmentation of the pipeline. A renewed focus on identifying where in Government our capabilities are in significant and growing demand has encouraged greater creativity and market shaping to exploit cross-selling opportunities across multiple agencies.

Continue to Shift Services to Higher-End Solutions

The Company has charted a clear path that leverages current capabilities and contract vehicles to allow greater access to customers requiring higher-end, higher value solutions. Specifically, our strategic emphasis on Software DME, particularly where we can apply our proprietary agile software development methodology, Cadence, and urgent US Army and US Air Force requirements for Cyber Protection and Computer Network Defense solutions contracted

through our NETCENTS 2 and ITES-2S contracts will allow us to enhance the value of the solutions we provide. This approach will also allow us to increase the amount and scale of higher margin work by broadening and deepening our penetration of currently under-developed customer sets through smart cross-selling.

Inorganic Growth

The Company intends to accelerate growth through acquisitions, and plans to build differentiated capabilities and new customers and contracts, with a focus on complementary, high-end technologies. We have established detailed plans to maximize leverage as a public company to accelerate growth through the acquisition of differentiated capabilities to achieve new customer penetration and enhance the sophistication of our offerings to existing customer sets. These plans include:

Utilize Existing M&A Pipeline

Since the completion of the business combination, we have continued to develop a significant pipeline of potential acquisition opportunities and attended a number of management presentations. Each opportunity is scrutinized with special consideration given to contract and/or customer concentration risk, the potential for cost efficiency synergies, additional and complementary capabilities, customers and contract vehicles, recent contract wins, and the quality of leadership and management.

Currently we are actively tracking more than 45 acquisition targets with revenue between \$40 million and \$100 million and EBITDA between \$5 million and \$15 million. In addition, we have broadened our pipeline to include more than 100 middle-market companies, with an active focus on around 20 of those at any one time. We continue to focus on companies with prime positions and strong past performance in the areas of software development and data analysis.

Add IP and Complementary, Differentiated Capabilities

The Company plans to target mergers and acquisitions opportunities with strong intellectual property and differentiated capabilities complementary to our platform, with a focus on high-end technologies that will scale and command premium valuations, including mobile application development, mobile technology systems, agile software development an