STATEMENT OF
JANE CHAPPELL,
VICE PRESIDENT, GLOBAL INTELLIGENCE SOLUTIONS,
INTELLIGENCE, INFORMATION AND SERVICES,
RAYTHEON COMPANY
before the
UNITED STATES SENATE
SELECT COMMITTEE ON INTELLIGENCE

—

March 7, 2018

Chairman Burr, Vice Chairman Warner, Members of the Committee, I am honored to represent Raytheon today before the Select Committee on Intelligence.

Raytheon and our employees understand — and take very seriously — our obligation to protect the Nation's secrets. We submit to the same clearance process that governs our Government and military partners, and we take the same oath to protect the information entrusted to us. Our number one priority every day is meeting the needs of our customers.

As Vice President of Raytheon's Global Intelligence Solutions mission area within our Intelligence, Information, and Services business, I navigate the disruptions that backlogs in the security clearance process cause every day — not just for Raytheon, our suppliers, and our industry peers, but ultimately for the warfighters, intelligence officers, and homeland security officials who rely on our products and services to protect the United States and our allies.

The magnitude of the backlog and associated delays speaks for itself. In September of 2017, the National Background Investigations Bureau (NBIB) faced a backlog of around 709,000 investigations. Delays in the initiation, investigation, and adjudication process for both secret and top secret clearances were two to three times longer than the timelines set by Congress in the Intelligence Reform and Terrorism Prevention Act of 2004.

But what those numbers fail to capture are the real-world impacts of the backlog. New careers are put on hold, top talent is lost to non-defense industries, and programs that will provide critical warfighter capabilities are delayed. And these impacts come with a real-world price tag, resulting in otherwise-unnecessary increases in program costs and inefficient use of taxpayer dollars.

We would gladly accept these costs if the clearance process delivered significant improvements in the security of our Nation's most sensitive

information, facilities, and personnel. Unfortunately, we have seen little evidence that the decades-old clearance process achieves that goal, especially when considering the threat posed by trusted insiders to classified computer networks. The modern threat environment can no longer be addressed using outdated and infrequent security snapshots.

To address the costs of the backlog, we ask Congress and the Executive Branch to implement fundamental reforms that streamline the clearance process and increase our Nation's security by leveraging advances in technology.

The Backlog

Raytheon is a technology and innovation leader specializing in defense, security, and civil markets throughout the world, and a world leader in advanced cybersecurity solutions for both the public and private sector. We have a workforce of approximately 64,000 employees, 68% of whom hold some level of security clearance. As these numbers demonstrate, Raytheon's ability to meet the needs of our customers depends on both our ability to attract and retain top talent, and our ability to get our employees the clearances needed to do their jobs.

With current backlogs, we have nearly 4,300 employees awaiting clearances, and almost 5,000 more awaiting the completion of a periodic reinvestigation — almost 15% of our total workforce.

In 2017, the average length of time it took a Raytheon employee to get an initial clearance was:

- 225 days for Confidential,
- 252 days for Secret,
- 500 days for Top Secret, and
- 328 days for Top Secret/Sensitive Compartmented Information (TS/SCI).

Surprisingly, the timelines for periodic reinvestigations were even longer, exceeding 615 days for a Top Secret clearance holder.

Our Missile Systems business has a rolling backlog of between 400 and 500 new hires who are unable to start their jobs because of delays in processing their clearances. And in the business unit I oversee, almost 300 software and systems engineers are also waiting.

These candidates have high-demand technical skills. They are enthusiastic about supporting our customers, and they meet the stringent pre-

qualifications we impose on anyone applying for a clearance. In short, they are "unicorns." We do what we can to keep them interested while they wait for their clearance, but a candidate's patience only lasts so long, especially when they have other options.

The Job Market

To truly understand the impact of clearance delays on the defense industry, you have to start with the job market. Our customers demand the most advanced technologies that Raytheon and the defense industry can produce — particularly on the most sensitive programs. This requires a continuous and persistent effort to recruit and retain top technical talent. And, our pool for positions requiring clearances is further restricted to U.S. citizens.

Faced with these customer requirements, the demand for cleared talent has dramatically increased. Currently, more than 120,000 job openings in the United States require a Secret clearance, and another 30,000 require a TS/SCI.

By our estimates, 480,000 people in the contractor community hold a Secret clearance, and 446,000 hold a Top Secret clearance. But most of these candidates are already employed, which means there are far more open roles than cleared candidates to fill them. This has led to a dire imbalance in the market for cleared talent. As a result, employers are paying cleared candidates an extra 10-15% in base pay and sign-on bonuses that *start* at $15,000.

In the last few years, non-traditional commercial competitors have also entered the market, driving these premiums to unprecedented levels. A recent example of this involved an entry-level software engineer who left Raytheon after receiving his TS/SCI clearance. A commercial competitor offered him a $20,000 sign-on bonus, a 15% increase in base pay, a 20% annual performance bonus, a $25,000 annual bonus for maintaining a TS/SCI clearance, and $20,000 in company stock.

And this offer was not a one-off. We often find ourselves choosing between matching these lucrative competitive offers and losing our cleared talent.

While preparing for this hearing, a Vice President from our missile business recounted a disappointing story. While he was pumping gas, he started a conversation with the gas station clerk, who turned out to be a recent college graduate who had accepted an offer to join Raytheon pending the outcome of his clearance. The candidate moved across the country to Tucson for his new job, but as his start date at Raytheon was delayed by the clearance process, he was forced to work at the gas station to make ends meet. While we are certainly proud he was willing to wait for the job of his dreams, many other

candidates are not as patient. And, when you add the pressing weight of college debt and the desire to keep technical skills current, the impact of delays on new college graduates is only amplified.

The impact of clearance delays is not confined to our highly-skilled technical workforce. They also affect candidates who we would like to hire for stable and well-paid manufacturing jobs. Many of these candidates come from lower- or middle-class backgrounds, and they simply cannot afford to wait — unemployed and without pay — for months while a clearance is received. Far too often, these candidates will accept another job well before we are able to bring them on following a months-long delay in the adjudication of even an interim Secret clearance.

To avoid stories like this, Raytheon often starts employees before they are cleared. They are assigned as much unclassified work as possible, but certainly not the kind of work they joined the company for, or what we hired them to do. And, while they wait, the associated overhead costs grow and grow. These costs ultimately work their way back into our products and services, eroding the buying power of our customers and delaying the delivery of critical capabilities.

Our subcontractors — particularly small businesses that cannot shift employees or other resources to manage their way through clearance delays — are also affected by the backlog. Recently, Raytheon identified a small, veteran-owned business to conduct a significant portion of the work on a sensitive Intelligence Community system designed to automate analysis for new sensors. After waiting through long delays to get their employees cleared, Raytheon was forced to give the subcontract to an alternative source to prevent program delays.

Even companies the size of Raytheon are not immune, and clearance delays have had real effects on our programs. To avoid the program delays and cost increases caused by the clearance backlog, we work diligently with our customers to leverage our cleared workforce across multiple programs to cover gaps.

These gap-filling personnel decisions — based primarily on clearance status instead of qualifications — have career consequences for everyone involved. High-performing employees can be stuck doing less important work, and program managers have to stretch cleared talent to cover critical tasks while the employee they need waits for a clearance.

Managing risk on our most sensitive compartmented programs or “Special Access Programs” (SAPs) is even more complicated because of the severe restrictions on the number of billets made available by the Government.

These restrictions can delay and limit workforce management decisions, and often prevent cross-pollination of lessons learned and efficiencies across our program portfolio. And reciprocity issues can sometimes prevent an employee with an active clearance at the same level needed on a different program from transferring between contracts without an additional investigation or adjudication.

These impacts negatively affect the lives of our employees, hinder Raytheon's ability to effectively manage complex programs vital to our national security, and add unnecessary costs that ultimately burden our customer's budgets and American taxpayers.

The Process

Despite various amendments to laws and executive orders, the security clearance process has gone largely unchanged since the 1940s. Applicants submit their background information and federal investigators (either federal employees or contractors) conduct an extensive investigation of the applicant.

Investigators operate on a five-tier system, with each successive tier mandating a more thorough background investigation based on the level of access granted. Tier 5 is reserved for the most sensitive access — to Sensitive Compartmented Information and other highly sensitive information or positions.

Periodic re-investigations are initiated, conducted, and adjudicated the same way as the initial clearance, and are required every 5 years for a top secret clearance, 10 years for a secret, and 15 years for confidential.

If the process looks complex on paper, I can assure you it is far worse in practice.

The intelligence reform act required each federal department and agency to honor the clearances of others (with certain limited exceptions) — a process known as "reciprocity."

In practice, agencies do not always honor the investigations or adjudications of others. Some mandate differently tiered investigations for different types of suitability and access determinations. Some mandate a polygraph. If a polygraph is required, the scope can vary. Some agencies mandate a polygraph every three years before a contractor can access sensitive government systems — even if the contractor has an active TS/SCI clearance that does not yet require a periodic reinvestigation. Some elements of larger departments do not acknowledge clearances issued by components within the

same department. And, when these differences arise, a new investigation is often ordered and added to the backlog.

And recently, at least one of our customers has mandated a Secret-level clearance for access to Unclassified/For Official Use Only (U/FOUO) material. These additional applications also clog the clearance pipeline, and impede clearance applications for individuals that require access to information that is actually classified.

Though we have seen some progress on reciprocity — particularly across the Intelligence Community — the Government continues to struggle with the size and scope of the issue. From our standpoint, the theory of reciprocity exists, but in reality, reciprocity is managed to different risk levels across different agencies. Simply put, the reciprocity ideal is not a fully realized practice. It is our understanding that Government-wide reciprocity standards originally planned for September 2013 have yet to be issued, are continually challenged with effective interagency coordination, and have no proposed deadline for completion.

The Government has only recently begun to automate and streamline the investigation process. In 2003, the Office of Personnel Management (OPM) automated the collection of information needed for the initial clearance application. Since then, OPM has made progress on a digitized SF-86 — the form applicants submit to initiate a clearance investigation or periodic reinvestigation — as well as other improvements to information collection and adjudication. However, following the OPM data breaches in 2015, at least one Intelligence Community agency stopped using these web-based tools. While OPM's overall efforts are steps in the right direction, none of them represent the transformative change needed to reduce the current backlog and prevent future delays.

Interim Reforms

The magnitude of the current backlog and associated clearance delays demands immediate and aggressive interim actions. Raytheon supports the Government's efforts to add investigative resources and ease requirements for periodic reinvestigations, and we also appreciate efforts to streamline the application process, automate and digitize certain information collection, provide for secure data storage, and improve other related processes.

Despite these improvements, at investigative resource levels NBIB has identified as feasible, GAO indicates that a "healthy" backlog — around 180,000 pending investigations — would not be reached until fiscal year 2022 "at the earliest."

As an interim measure, Raytheon encourages the Government to reevaluate the "first-in/first-out" investigation approach and adopt a risk-based method that would quickly adjudicate low-risk investigations and prioritize mission-critical investigations. Higher-risk, time-consuming investigations would be delayed until additional investigative resources were available.

Adjusting the periodic reinvestigations process will also free investigative resources for initial reviews, but we urge the Government to reconcile the current extensions with inconsistent recognition of "expired" clearances. Despite a December 2016 Department of Defense (DoD) memorandum directing otherwise, employees with current, valid investigations are being denied access by some customers based on Government-directed delays to initiate a periodic reinvestigation. These inconsistent decisions exacerbate the backlog with no clear risk-based justification.

The Government should also consider recognizing background investigations conducted by private sector employers as the basis for lower-risk clearance and access determinations. Consistent with applicable laws, these employment-related investigations often entail the collection and review of publicly available and sensitive information on a candidate's financial, criminal, residency, military and educational records. These records serve as the foundational components of all federal clearance investigations. If these investigations met Government-established standards for rigor, the results could serve as the basis for certain lower-risk clearance, access, or suitability determinations by an adjudicating agency.

Additional resources and thoughtful adoption of low-risk interim adjustments may marginally improve the current situation, but fundamental reforms to the clearance process are essential. Without these foundational efforts, inefficiencies will continue to frustrate progress with no real increase to the security of the Government's information, facilities, or personnel.

Fundamental Reforms

In 2006 — with a clearance backlog of 300,000 investigations — a coalition of industry associations recommended a set of reforms known as the "Four Ones" (https://www.itic.org/public-policy/SecurityClearanceReformCoalitionWhitePaper%28Final%292006.pdf and https://oversight.house.gov/wp-content/uploads/2017/10/ITAPS_Hodgkins_Testimony_Security-Clearance-Investigations.pdf).

- One Application — one standardized and digitized application for all clearance determinations, updated continuously and stored securely,

to form the "permanent digital record" for the initial and any subsequent suitability, access, or clearance determinations.
- One Investigation — enabling a dynamic, ongoing examination of individual risk by implementing continuous evaluation.
- One Adjudication — streamlining and standardizing the overly complex adjudication system so that one agency's clearance decision is respected by other departments and agencies, promoting reciprocity and efficiency.
- One Clearance — recognized across the entire Government, transferable from department-to-department, agency-to-agency, and contract-to-contract.

More than a decade after they were first proposed, the "Four Ones" continue to serve as a roadmap for needed reforms, and a reminder that progress has fallen far short of expectations.

To make immediate progress, Raytheon encourages the Government to prioritize and set incremental milestones for implementing Government-wide reciprocity, continuous evaluation, and information technology reforms.

Information technology reforms that enable automated application collection, incorporate new information derived from investigations or continuous evaluation, and provide secure, cross-domain mechanisms for accessing investigative information are vital to support each prong of the "Four Ones." Technology forms the basis for automated applications and the establishment of a permanent, electronic investigative file. It underpins continuous evaluation, and is necessary to provide the confidence departments and agencies need to confidently implement Government-wide reciprocity.

We support the direction that the Department of Defense (DoD) and the Office of Personnel Management (OPM) are taking to establish the National Background Investigation System, but vigorous oversight and robust resources will be required to address integration and security risks that the system must overcome.

Effective implementation of a comprehensive continuous evaluation program will help eliminate the need for time-based periodic reinvestigations for all clearance holders, cutting the unnecessary costs incurred to fully investigate even low-risk individuals. More importantly, we strongly believe that this dynamic, ongoing approach to vetting will increase security and detect, deter, and mitigate insider threats.

As currently constructed, the periodic reinvestigation system only provides a risk snapshot for clearance holders when the initial investigation is conducted and at prescribed 5-, 10-, or 15-year intervals. In the intervening

periods, our Nation's security relies upon self-reporting and serendipity to identify risks.

Continuous evaluation fills this security gap, providing immediate reporting on security threats and allowing agency security officials to make real-time risk determinations. When necessary, these risks may be so significant that immediate personnel action is required. Alternatively, the risks may call for initiation of a risk-based, aperiodic reinvestigation. Any aperiodic reinvestigation, based on the continuous collection of investigative data since the initial clearance determination and informed by targeted investigations associated with significant security concerns, could be conducted more efficiently than the current process which basically recreates the initial investigation.

I would be remiss if I did not underscore Raytheon's belief that an effective continuous evaluation system must be accompanied by robust user activity monitoring (UAM) programs. With so much sensitive information contained in our Government's information technology systems, it is vital that security officials be able to quickly identify inappropriate user activity on their networks — both classified and unclassified. Context-aware UAM programs, when combined with data from other continuous vetting sources, will enable real-time, risk-based decision making about system users and clearance holders.

One tool informs the other, *and the combination promotes increased privacy protections*. Comprehensive, detailed monitoring of all users is unwieldy, impractical, and invasive. Modern, analytics-enabled UAM allows security officials to adjust the sensitivity of the tool based on the risk associated with particular users. So, a clearance holder with security risks identified in continuous evaluation could be more carefully monitored by UAM when using Government systems. Users with low-risk activity on Government systems may require less comprehensive continuous evaluation. The combination promotes efficient targeting of investigative resources toward higher risks, and protects the privacy interests of low-risk personnel or contractors.

The electronic availability of secure, up-to-date investigative records, clearance histories, and any security risks identified through continuous evaluation and UAM, should make the implementation of reciprocity that much easier. Agencies will be more willing to trust prior adjudications and will have access to any intervening derogatory information — not to make independent clearance decisions, but to promote a one-Government/one-individual approach to the clearance process.

Finally, I believe it is critical to note that sustained and relentless leadership — from both Congress and the White House — will be crucial to successfully implement reforms. Even the most well-intentioned reporting requirements, working groups, and legislative deadlines have not, and will not, outlast the fear of change or the comfort of the status quo.

The Committee's investments of time and resources to effectively implement this security framework will help eliminate the investigative inefficiencies, duplication, and stove-piped decision making that hamstring the current clearance system. They will promote the effective and dynamic recruitment, retention, and deployment of Government employees and contractors as dictated by skill and performance, not based merely on the availability of a current clearance. And, critically, they will help close the security gaps that threaten our Nation's secrets and personnel.

Thank you for the opportunity to be here today, and I look forward to answering any questions you may have.

****