LEVERAGING EMERGING TECHNOLOGIES IN THE SECURITY CLEARANCE PROCESS

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

SECURITY POLICY REFORM COUNCIL

MARCH 2014

INSA

ACKNOWLEDGEMENTS

INSA CHAIRMAN
Ambassador John Negroponte

INSA SENIOR INTELLIGENCE ADVISOR
Charlie Allen

INSA SENIOR NATIONAL SECURITY ADVISOR
Ambassador Bob Joseph

INSA STAFF
Ambassador Joe DeTrani, *INSA President*

Chuck Alsup, *INSA Vice President for Policy*

Jeff Lavine, *INSA Director of Administration & Management*

Nate Brown, *INSA Fellow*

Kelly Evans, *INSA Intern*

SECURITY POLICY REFORM COUNCIL (SPRC) LEADERSHIP **
Charlie Allen, *INSA; Chertoff Group*

Kathy Pherson, *Pherson Associates, LLC*

SPRC'S SUBCOMMITTEE ON CONTINUOUS MONITORING AND EVALUATION **
Mitch Lawrence, USIS (Subcommittee Chairman)

Kathy Pherson, Pherson Associates, LLC (SPRC Oversight)

Tabetha Chandler, Facility Technology Services, Inc.

Edie Curry, Palaxar Group, LLC

Bill Davidson, KeyPoint Government Solutions

Art Davis, Booz Allen Hamilton

Linda Dei, ASM Research

John Ellingson, Skeptical Systems

Judith Grabski, Thomson Reuters Special Services

Bob Harney, ManTech International

Darrell Lloyd, The SI Organization, Inc.

Adam Lurie, Social Intelligence Corp.

Fred Riccardi, ManTech International

Charlie Sowell, Salient Federal Solutions

Individual contributions/attendance by Army, CIA, DSS, NCIX/ODNI, NSA and USD(I)

APPENDIX WRITING TEAM
Randy Fort, Raytheon Company (Principal Author)

Adam Lurie, Social Intelligence Corp.

COPY EDITOR
Beth Finan

EDITORIAL REVIEW
Joe Mazzafro, Computer Sciences Corporation

*** Participation on the Council or Subcommittee does not imply personal or official endorsement of the views in the paper by any members or their respective parent organization(s).*

INSA SUPPORTS A HEALTHY PLANET

INSA White Papers are printed on recycled paper that is 50% recycled content including 25% post consumer waste.

> We have a unique opportunity to make long overdue adjustments to the security clearance process.

EXECUTIVE SUMMARY

True reform in national security clearance processes over the past 60 years has been rare. One of the best examples of real change has been the recent shortening of security clearance timelines in line with the requirements of the Intelligence Reform and Terrorism Prevention Action (IRTPA) of 2004. Despite these accomplishments, security breaches by clearance holders like Bradley Manning, Edward Snowden, and Aaron Alexis point out the need to focus on the periodic reinvestigation (PR) process and demand even more fundamental and beneficial improvements based on three key drivers:

- Recognition of a **compelling need** to evaluate clearance holders' compliance with security requirements on a more regular basis using broader sets of data.
- Expressed **determination by leaders** in institutions ranging from the Intelligence Community (IC) to the Department of Defense (DOD) to the Office of Personnel Management (OPM) to Congress to take concrete action and do it quickly.
- **Innovations in technology** and data processing that provide options for affordable solutions to handle a larger volume of data and subjects with better quality results.

This confluence of factors presents a unique opportunity to make long overdue adjustments to the periodic reinvestigation component of the security clearance process. Besides giving security and operational managers better insights into potentially dangerous changes in the life circumstances and environments of those entrusted with sensitive and classified US Government information, well-designed alterations also have the potential to remedy many of the limitations that have plagued the clearance process for decades. These include:

- Resolving the dilemma in current policy that sets timeframes for reinvestigations that cannot be met, particularly during times of constrained resources.
- Taking advantage of investigative resources now technologically available at low cost that may contribute to the adjudicative quality of PRs.
- Fostering reciprocity across agencies of clearance holder information affecting contracts, mission support, and costs.

This report outlines an approach to augment PRs through a process of "continuous monitoring and evaluation" (CME) that will make reinvestigations more regular and consistent; improve the relevance and accuracy of PR data collection and analysis; and enable greater portability of clearance holder data. Our combining "continuous monitoring" and "continuous evaluation" into a single term, CME, is intended to emphasize our belief that workplace information technology (IT) use behavior and external personnel data can and should both be defined as inputs to a continuous monitoring process. Current directives define the terms separately (see Glossary).

An "enhanced PR" does not replace the current PR process, but offers an evolutionary way to implement a state-of-the-art process to provide an ongoing perspective on cleared individuals rather than a snapshot every five years or more. It:

- Incorporates data collection applications and techniques offered commercially;
- Establishes a common means to collect and securely store user unclassified information on required submission forms, such as the Standard Form (SF)-86, SF-85P, SF-86C, and e-QIP;
- Adjusts the methodology for reviewing, analyzing, and acting on collected information so that investigators and adjudicators have a context and framework for understanding the data;
- Supports and complements other Government security reform efforts, most notably the Director of National Intelligence's (DNI) seven goals for security policy reform; and,
- Helps identify changes in the situations of an individual's life that might suggest early interventions and forestall later difficulties.

An enhanced PR process that merges CME capabilities with current PR requirements and goals will produce:

- Continuous updating and near real-time reporting of results, flagging behavior that may prove to be inconsistent with a security clearance or job assignment.
- Better informed risk-management decisions and more opportunities for mitigating and resolving clearance holders' problems.
- Increased accuracy of security clearance holder information by validating and evaluating reported or unreported information and resolving errors and omissions that may adversely affect the individual.
- Higher confidence in investigation analysis due to more relevant, time-critical, and up-to-date data being reported.
- A universal data gathering mechanism that facilitates reciprocity of clearance information.
- One means for security clearance holders to meet all reporting responsibilities without duplicative submissions.

Interested in continuing the conversation?

Send your feedback to comments@insaonline.org, and cite the name of this INSA White Paper in the subject line.

PROBLEM: MODERNIZING A REINVESTIGATION PROCESS BUILT FOR THE LAST CENTURY

The emphasis in security reforms during the past decade has been on reducing initial clearance processing times and speeding our ability to clear those needed to protect our nation from those seeking to do it harm. The Director of National Intelligence (DNI) and officials in the Department of Defense (DOD), the Office of Management and Budget (OMB), and the Office of Personnel Management (OPM) have accomplished a great deal, but the push for new clearances has left the reinvestigation process lagging behind. The resulting gaps between policy and reality in contractor reinvestigations, for instance, explain many of the disconnects between the security and acquisitions processes identified in INSA's earlier paper, "Next Steps for Security Reform."

TECHNOLOGY GIVES US CHOICES

Would you rather see photographs every five years of family members or have live video access to them via FaceTime or Skype twenty-four hours a day?

The current reinvestigation system is challenged because:

- Its funding is usually ranked below initial clearances and other priority programs. Few agencies have been able to maintain the resources for consistent five-year reinvestigation programs.
- Individuals, both government and contractor, move more rapidly among programs, sponsors, and missions; this leads to duplicative and overlapping entries in the clearance process and forces them to spend time filling out the same forms for different agencies.
- Multiple agencies collect the same data in stovepiped implementations of the SF-86 and other forms that limit sharing, increase the potential for information to be missed or overlooked, and make it more difficult to identify and take into account new data and indicators of changes in an individual's life. Some agencies ignore, fail to look at, or lack access to other agencies' data; this at best slows reciprocal processing of "crossover" clearances among agencies, but at worst allows for new accesses without full consideration of meaningful personnel security data.
- Reciprocity among agencies—despite some improvement—is still highly inconsistent and at times fleeting. This is particularly significant for industry, which provides services across the national security community and comprises well over 60 percent of clearance holders.

The Impact of Societal Change on Personnel Security

The traditional focus for background investigation information has evolved over the past 15 years to adjust to a world that is far different from the one in which the investigative standards were established more than 50 years ago.

The cultural migration to online community life is moving us from secrecy to transparency and even impacts our understanding of honesty and deception. Portrayals of Manning and Snowden as "freedom fighters" rather than threats to national security argue that effective screening of persons under oath to protect classified information is more important than ever. Knowing that spies on average since 1947 began committing espionage after about 12 years of service is evidence the PR continues to play a vital role in verifying security clearance holder trustworthiness and loyalty.

The online world brings substantial opportunity for cost savings and efficiency. Investigators no longer need to rely primarily on interviews to find out where a person travels, what they like, who their friends are, what they buy, where they live, and what interests they have. Each of us has a "digital exhaust" or footprint whether we like it or not. Unlike interviews, records can be more easily verified and collectively analyzed for even insignificant changes. This data enables targeted interviews and expands potential interviewees.

The security offices within the intelligence and defense communities are acutely aware that the reinvestigations systems have not kept pace with those for initial clearance processing and that the IRTPA emphasis on speed has created pressures that can impact quality. They are moving to readdress, adjust, and improve the "state-of" PRs to preserve the investment in a trusted workforce after initial screening. Up-to-date reinvestigations are essential to clearance reciprocity. One agency's inability to meet reinvestigation standards limits holders of its clearances from working elsewhere in the IC without shifting the burden of the reinvestigation to the receiving agency. Reinvestigation programs are rarely ever fully funded to meet the traditional five-year standard, which lacks empirical data to support it, and are among the first to fall victim to budget cuts by being either severely delayed or totally stopped.

Overtaking the age-old funding issues, however, are concerns that the PR has not kept pace with generational and lifestyle changes and the available data and technologies that provide insight into today's workers. The INSA paper "The Future is Now: Assessing the 'ePersona' in Background Investigations" (see Appendix) cites a staggering percentage of the population who "live" online and do not have that aspect of their lives reviewed as part of the current PR clearance policy. No standard exists for a "neighborhood check" of the "online neighborhood," which is without a fence line and extends beyond national borders and languages. The geographic neighborhood will always remain part of the PR, but information contributing to the "whole person concept" review occurs online and is being missed.

These same lifestyle changes and technologies actually make establishing a set period for review of five, seven, or more years irrelevant and potentially even detrimental to national security. The commercial technology and data exist today for a continuous assessment of anyone holding a security clearance that provides a frequent, continuous "whole person" "video stream" rather than a five-year "snapshot."

Deeply disturbing national security incidents, like the Fort Hood shootings, Wikileaks, the Snowden case, and the Washington Navy Yard shootings—all involving security clearance holders—cast a growing shadow on a PR process that does not incorporate emerging data sources, collection capabilities, automated analysis tools, and the "ePersona." Better information, more frequent reviews, and refined analysis of clearance holder data will increase the probability that those perpetrating grave harm may be interdicted prior to their actions.

SOLUTION: ENHANCING THE PR WITH CONTINUOUS MONITORING AND EVALUATION

Incorporating up-to-date sources and technologies can enable an evolution of the PR process to operationalize a continuous monitoring and evaluation (CME) capability that would constantly evaluate critical factors and behaviors and facilitate informed and prioritized PR processes. This enhanced PR process would take advantage of current and continually advancing technology to bring together and constantly monitor and update the masses of "big data" relevant to cleared populations and the clearance process. In much the same way credit, insurance, health, gaming, and other high security industries "clear" their staffs and clients, clearance and investigative data can be synthesized in like categories to allow agencies to continuously monitor use and evaluate changes in the cleared populations at all levels.

This amalgamation of information provides great opportunity to exploit more effectively and consistently public data sources from social media and the internet as a whole to create the "image" and "chronology" of a person. The patterns of risk and behavioral indicators can be combined with existing government data sources. Indicators and thresholds can be customized to address the range and types of cleared personnel, including the "privileged user" and other high-risk positions critical to national security. Adjudicators can be trained in risk management and structured analytic techniques to weigh sources and data against potential scenarios of concern.

This process needs to be approached with care to ensure that adverse information is verified to protect individual rights, individual agency information is protected, and strong configuration controls are in place. An enhanced PR process can leverage work in Intelligence Community programs on data sharing, such as IC ITE, to ensure that sharing of security information is in line with processes and procedures for other sensitive intelligence data.

An enhanced PR process must link closely with counterintelligence and Insider Threat Detection and Prevention Programs. The public online data sets are rich targets for adversaries conducting their own form of offensive CME to exploit US clearance holders and spot potential recruits to commit espionage. The information is so easily available that even friendly nations will use free and legal online sites like Black Book Online and Public Records Online for their due diligence.

An enhanced PR process and the Insider Threat programs are mutual reinforcements in achieving the goal of constant verification and evaluation of trust required for personnel security, counterintelligence, data integrity and reporting, and reciprocity. This type of data collection, merging, and analysis is already being accomplished at varying levels of efficiency in existing programs (see, for example, INSA's report on "Insider Threat Programs in the US Private Sector"). Patterns of information systems abuse, information mishandling, and other indicators are being merged with sets of behavioral indicators that include human resources, counterintelligence, travel records, financial changes, life changes, and criminal issues. Working together will enable government agencies to make the best use of scarce resources to include PRs as a priority concern, improve reciprocity, and detect potential problems as early as possible.

HOW IT WOULD WORK

We envision an enhanced PR process as a continuous collection and assessment capability derived from all sources undergoing constant analysis of relevant data. It is not a behavior prediction methodology or tool. It monitors relevant uses and behaviors, specifically anomalies that are indicators of inconsistent behavior based on newly discovered information. When behavior is detected straying from that clearance holder's responsibilities and history, it is then observed and analyzed. If warranted, solutions to mitigate or intercede are addressed.

The current core PR process would not change, but would be carried out only for specific reasons, such as reported issues, discrepant CME corroboration and evaluation, or the setting of a new period of time for its mandatory use. The CME enables pushing back the current five-year PR goal to seven, ten, or even twelve years. The year goal chosen could be consistent with and adjustable to the mean period experienced in "time-until-espionage" statistics cited earlier, the agency's preference, or its ability to fund more frequent PRs.

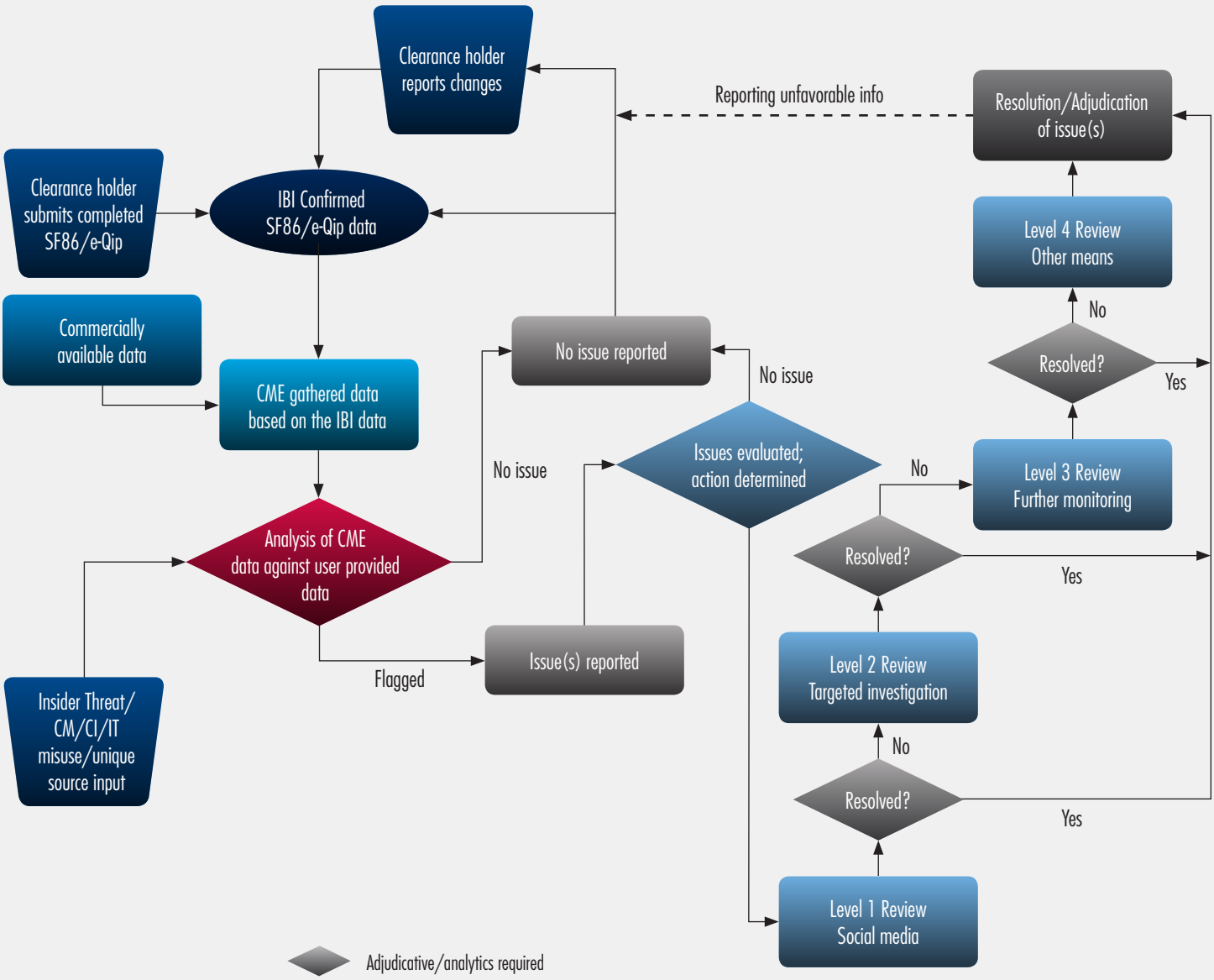
The CME baseline for a clearance holder (see Figure 1) is derived from the SF-86/e-QIP data confirmed during the Initial Background Investigation (IBI). Cleared personnel update their personal history as it changes from marriage to foreign travel, medical issues to financial, and other changes as required by reporting guidelines. One means of providing these updates could be through a form like the SF-86C, which is a quick method some organizations use on a yearly basis for standard reporting of changes that reminds clearance holders of the importance of reporting and cautions them about the consequences for falsification.

THE CME PROCESS IS LIKE TRIAGE

In an emergency room, changes or problems with the data known about healthy patients determine the actions needed to return the patient to good health. Information is gathered, charted against past history, investigated, and analyzed by experts, and then action is taken or not taken. Everything from aspirin to open heart surgery is available for consideration on a 24/7 basis and administered by the proper physician and team.

The CME process enables the gathering of external information from hundreds of commercially-approved databases, which is then charted against the baseline SF-86/e-QIP data, other internal agency databases, and checks on the "clearance health" of the clearance holder. Adjudicators respond to discrepancies, determining whether to monitor more closely, intervene, or fully investigate the flagged issues. The determination methodology is already established by each agency through the thresholds currently used for adjudicative decisions. The flow and frequency of data in the CME process should enable many of the thresholds to be automated to assist a human adjudicator making the call for minimal or more drastic action.

Figure 1: Enhanced PR "Triage"



By flagging the triggering event as it happens and bringing it to the attention of the monitoring authority, CME requires an action be recorded and an audit trail created. CME provides a pathway linking that event with any other events that have been or will be monitored, providing the previously missing context against which the complete, holistic aggregation of events can be assessed. The knowledge that an audit trail exists should allay adjudicator fears about reporting the event up the chain of command because it will be relayed within an appropriate context.

The driver behind the success of CME and ultimately an enhanced PR process would be the establishment of an online application and resultant database to replace the paper and online SF-86, SF-85P, and SF-86C. This capability could create a centralized database from which all agencies could access clearance holder information, review changes in real-time, see investigative status and "flags" immediately, and enable portability of clearance eligibility. Establishing an SF-86 management tool and data repository will depend on a system design that incorporates the best possible security standards to protect individual agency sensitivities as well as the massive amount of Personally Identifiable Information (PII) and security data. The concept provides:

- A mechanism to track costs for clearance-processing services at the national level. For example, submitters would assign agency designators to their submissions to enable tracking the number of submissions per agency and aid allocation of national level funding for each agency's clearance processing services.
- Timely and improved self-reporting of life changes in one location for access by multiple agencies. Cleared contractors receive different directions from each government agency to report changes to their personnel security information; these include agency-specific forms, emails, entries only on classified systems, duplicative reporting during the PR process, and multiple SF-86s or SF-85Ps. Clearance holders are frequently confused whether to report information only to the Defense Security Service (DSS), the agency or agencies holding the person's clearance, or just to the agency or agencies. Invariably the contractor is held accountable for not divining the correct path or method. Once the report is submitted, the information gathered by one agency is generally not distributed among others and, if it is, sharing is not timely.

A secure, centrally managed, self-reporting web portal will save time and expense managing the different processes and formats. The website could have a menu for the clearance holder to report required life changes such as marriage, divorce, foreign travel, financial disclosure information, and foreign contacts. Clearance holders would be accountable for keeping their information up-to-date. Current PR data would be readily available and accessible for use with enhanced PR continuous monitoring and evaluation.

ADVANTAGES OF AN ENHANCED PR PROCESS

- An enhanced PR could fill the gaps in the data collected by the current PR process, which has no or minimal collection standards or comprehensive review and evaluation of the "ePersona" of clearance holders. The abundance of accurate and valid data not currently reviewed and analyzed is significant. Filling those gaps could lead to a better quality investigation and "whole person" adjudication.
- CME adds context for what previously might have been viewed as an isolated event and a single violation of policy. By helping place triggering events in a larger context, it assists in making the best decision possible at the time and provides the audit trail for complete and appropriate accountability. In virtually every after-action analysis of the notorious cases of espionage or significant security failures that might be addressed by CME, we have instances of policy failures in which some event was noted and reported and ultimately either ignored or misinterpreted. With the benefit of hindsight analysis, that event is frequently seen to be a potential contributing factor that, if seen in context, could have led to prevention of the ultimate consequence.
- The data will also allow for more detailed and deeper analysis. For example, currently developed references (DRs) as part of the PR can be a challenge for an investigator in getting to "know" the subject. CME will automatically cross-reference names within the security clearance holder database as well as what is available online. The investigator will see a veritable genealogy of contacts for each subject.
- CME will allow for near real-time evaluation of collected information using a combination of automated thresholds, analytic tools, user input of changes, and heuristic alarms, flags, and notifications to provide the adjudicator the available data to make risk assessments immediately. This will eliminate the reinvestigation gaps and more than likely allow for intervention with clearance holders who may be trending toward known behavior that may jeopardize their clearance, threaten national security, or harm themselves and others.

- The system will notify clearance holders when non-issue updates are detected to verify the update and explain why they did not update earlier. This type of "accurate" and "up-to-date" monitoring will not only simplify the process but serve as a deterrent to the subject. When clearance holders know that information about them is continuously updated and evaluated without benefit of their input, they will either self-report honestly or attempt to hide the changes. The deceptive behavior will be easier to detect.
- Counterintelligence officials will benefit from the additional information on clearance holders that will give them a better platform from which to prevent, mitigate, or intervene in behavior inimical to national security.

> Enhanced PR could fill gaps in the current PR process leading to a better quality investigation and 'whole person' adjudication.

- CME analysis can be linked with information technology Insider Threat detection capabilities to obtain a full view of the clearance holder's personal accountability as well as work activities.
- The online clearance information reporting application resolves a number of current problems inhibiting reciprocity of security clearance information, including tracking costs of the security clearance process, simplifying reporting of clearance-relevant information, providing common access by government agencies to basic clearance holder information, enabling the clearance holder to be accountable for reportable information, and providing the baseline from which to conduct continuous monitoring and evaluation.
- Specifically, an enhanced PR process will eliminate costly complexities introduced into the acquisition process that require active clearance holders proposed for new opportunities to be within the artificial five-year investigative scope. This solution improves reciprocity across the IC, including special access programs (SAPs), and reduces the risk that trustworthy industrial contractors with active clearances and valuable skills will be delayed or put out of work for the wrong reason.

ISSUES FOR DISCUSSION

An enhanced PR process, like any change, presents issues to be considered and options weighed before deciding on the optimal course of action for the time, circumstances, and resources available. We anticipate the need for full discussion of issues such as the following:

Legal Considerations. The open source or online data involved in CME is all public information. Commercial entities engage in continuous monitoring every day; it is legal with even fewer restrictions when the information indicates possible fraudulent or deceptive activity. Types of data legally available include car, military, buyer, collections, credit, demographics, taxes, insurance, permits, employment, fraud, banking, liens, judgments, health, geolocation, consumer reports, academics, corporate holdings, public records, phones, postal service, real estate, airlines, warranties, and charities.

Privacy Issues. An enhanced PR process would follow the same principle for data gathering that exists today—the clearance holder's release authorization. The government is legally able to ask a candidate to sign a release authorizing access to personal information during the investigative review. Online access to the same data is covered in the release. Legal reviews and cases are still evolving with online "privacy." The line currently drawn—based on outcomes of court cases in two states—prohibits requesting UserID and passwords to personal sites.

Interagency Agreements. An enhanced PR process represents the next step forward in building reciprocity and consistency in security processes. Technology interoperability, initiatives such as IC ITE, and the recognition that many in the cleared population do not spend their careers in one agency's stovepipe set the stage for a common agreement among government agencies to adopt an enhanced PR process and foundational online clearance information reporting application. Independent agency implementation complicates information reciprocity and efficient use of valuable resources. The system design must take into account critical exceptions in information and identities that some agencies process and maintain separately, but in complementary formats that allow for seamless transition of those identities into the main system, if appropriate.

Technologies and Tools. A number of companies have already taken on the challenge of using public data sets and social media to characterize individuals; this is what the DNI refers to as CE. Others have focused on recording their keystrokes, file accesses, and other electronic behaviors in the workplace, which the DNI characterizes as CM. Implementing an enhanced PR program effectively requires not just picking one or two applications, but a careful understanding of how technologies and tools can fit together to cover the entire process that we are calling CME. The system needs to be scalable and modular to accommodate future innovations or changes in our knowledge of individuals, behaviors, and data sets.

Resources, Cost-Benefit, and Metrics. An enhanced PR process will require changes to and review of current funding processes and budgeting. A cost-benefit analysis should underlie requests for resources and meaningful metrics should be defined in advance that will gauge qualitative improvements as well as those that are more easily counted, such as quantity and time. These are the cornerstones of a compelling programmatic justification that will convince budget reviewers, authorizers, and appropriators to provide funding needed to design and implement an enhanced PR process.

Preparation of Investigators and Adjudicators for CME Success. One of the greatest impacts of an enhanced PR process will be an initial tidal wave of conduct identified through CME that was not previously reported or discovered and will require investigation and adjudication. Most agencies have experience handling increased information flows when reinvestigation programs are funded to "catch-up" on backlogs, but this new set of data will present additional challenges. Government and industry investigators and adjudicators will need to be trained for targeted investigations of flagged issues that will require deeper understanding of finance, legal, health, and drug issues. They will have to weigh ambiguous and contradictory data and be accountable for making analytic judgments that are consistent and replicable.

Implementation Details and Implications. Implementation will raise a variety of new questions to be addressed, including some like the following:

- How will candidates and clearance holders respond to comprehensive monitoring?
- Who "watches the watchers" of the clearance holder database? How are data verified, tracked, and audited?
- An enhanced PR process encourages clearance holder accountability and proactive reporting. Will the increased reporting have an impact on government systems or how security offices handle clearance holders who work across projects and agencies?
- What new contracts requirements will be generated and how will they impact the system?

RECOMMENDATIONS

An enhanced PR solution does not rest with one organization or product, just as no one organization possessed a Saturn rocket, landing module, or computer programming to reach the moon at the time of President Kennedy's speech in 1962. Government and industry will need to work together to craft an enhanced PR process that is adaptable but universal; accessible but adequately secure; and actionable but still timely, relevant, and cost-effective. We envision a team of companies working with the full range of government agencies to get an enhanced PR process "to the moon and back."

> Why settle for a review every five years or more when one can be available on a recurring basis?

1. INCORPORATE AN ENHANCED PR INTO THE SECURITY CLEARANCE PROCESS.

Adding an enhanced PR to the existing security clearance process will ensure near real-time changes about a cleared person are captured and evaluated on a much more frequent and reliable basis. The ability to monitor and evaluate "living" data on such a recurring basis allows for a more realistic "whole person concept" of a cleared person's habits and life changes. Why settle for a review every five years or more when one can be available on a recurring basis? Continually assessing real risks associated with clearance holders' access to classified materials systems will improve the government's ability to identify and mitigate changes and vulnerabilities before national security compromises.

2. MOVE TO AN ONLINE CLEARANCE INFORMATION REPORTING APPLICATION

The cost and time saving of this application will be recognized across government as a centralized clearance repository that provides instant access to the most current data for investigations and adjudications. Redundancies can be eliminated and old or irrelevant data archived for "whole person concept" evaluation and risk assessments of contradictory or inconsistent patterns. Universal portability of clearances and credentials will enable clearance holder expertise to be easily and quickly leveraged across sensitive programs to meet pressing mission needs, but without losing visibility into life changes that might jeopardize sensitive information. From the industry perspective, a streamlined, online clearance information reporting service will eliminate many of the complexities that result from having cleared staff members who contribute their expertise to programs across multiple agencies.

3. MAKE USE OF INTERNAL AGENCY DATABASES

Along with the database derived from the online reporting application, each agency should be able to link this enhanced PR evaluation to its internal databases. For example, each agency typically maintains data relevant to a clearance holder for performance appraisals, foreign travel, financial disclosure data, operational assessments, deployment decisions, medical background, counterintelligence, access determinations, and self-reporting requirements. Most agency legacy systems and accountability processes maintain this information in owning division "stovepipes," such as security, human resources, medical, recruiting, general counsel, and operations. It is often only accessible when requested or after an issue arises, which is almost always too late to head off a developing vulnerability.

4. USE AN ENHANCED PR TO TARGET HIGH-RISK CLEARED POPULATION

The central use of self-reported data will allow agencies to maintain risk profiles for all clearance levels and set escalation flags matched with levels of clearance access. This could help when staff members are cleared at multiple levels on differing contracts or at multiple agencies. Risk markers can also be set as one person gains access to multiple, classified networks or other advanced caveats. Automated analytic tools can help investigators and adjudicators matrix or triage the dataflow and analysis to focus on "at risk" personnel, comparing enhanced PR-derived information against self-reported data within the context of any special, program-unique, compartmented, or agency-mandated "at risk" thresholds. Identified differences can lead to more rapidly generated risk assessments and mitigations, including issue-targeted investigations that would be scheduled immediately rather than waiting until a five-year reinvestigation. An enhanced PR complements and expands the current targeting of "privileged users" by providing a continuous aspect to monitoring their publicly available personal information.

5. LEVERAGE AN ENHANCED PR AS A DETERRENT AND ACCOUNTABILITY BOOSTER

An enhanced PR through the online reporting application will make it easier to self-report personnel security-relevant issues and encourage individual accountability because clearance holders will understand the CME capabilities to uncover errors or omissions. We believe clearance holders will be more careful, accurate, and timely in reporting foreign activities, finances, legal issues, and relationships in an easy-to-access system that enables them to do it once, see the context of what they have reported previously, and use formats that are consistent from one time to the next. Automatic reminders and other mandatory reporting periods can be established for recurring requirements, such as periodic financial disclosure reporting. The self-reported data can be verified and compared with publicly available data, providing a near real-time check on clearance holders' honesty in self-reporting.

An interim measure might be to make greater use of "randomness" as a solution. Like random drug testing and Internal Revenue Service audits, random checks encourage clearance holders to self-report if they are aware of the chance they can be evaluated at any time. This may discourage unwise behavior in the first place or at least cause clearance holders to act with caution if they know they are being continuously monitored and can lose their jobs.

6. PARTNER WITH THE INSIDER THREAT AND COUNTERINTELLIGENCE EFFORTS

The ability to better track tendencies and changes in near real-time and from a broader range of data sets is invaluable to personnel security, counterintelligence, and Insider Threat programs. Combining an enhanced PR with Insider Threat continuous monitoring of IT access provides information essential to evaluation and targeting in all three programs. The vast comparative data produced from an enhanced PR could revolutionize counterintelligence by providing broader access to data that counterintelligence

officers can use to spot behavior, travel, contacts, and purchases across personnel, contracts, assignments, and supervisors worthy of investigation. Espionage post mortems could benefit from pre-mortem assessments that might identify suspicious behavior in time to deter or interdict illegal activities.

7. IDENTIFY A PROOF OF CONCEPT POPULATION

An enhanced PR "proof of concept" population should be the "Tier 5" or "SCI" accessed clearance holders. This group comprises only four percent of the nearly 5 million clearance holders, represents the most complex of the clearance processes, and contains the population that can do the most damage to national security. Demonstration of success with this small but critical population may provide an easily translatable template for the remaining 96 percent of clearance holders.

8. SET EXPECTATIONS WITH A COST-BENEFIT ANALYSIS, METRICS, AND TECHNOLOGY STANDARDS.

A best practice of good analysis is to take time to stop and reflect about expectations for tangible benefits of new initiatives and what "success" looks like. Cost containment depends on understanding the relationship between the costs and the expected benefits. Achieving reciprocity gains early on depends on defining technology standards and a transition path to the incorporation of an enhanced PR process. Early articulation of the problems agencies may face in adopting new systems and applications should make it easier to accommodate exceptions in ways that are compatible with the general solution.

9. START EARLY TO TRAIN INVESTIGATORS AND ADJUDICATORS TO BE PREPARED FOR NEW WAYS OF DOING BUSINESS.

Developing the skilled workforce to create mental frameworks for new and additional information, weigh ambiguous and contradictory indicators, and justify potentially life-changing decisions about individuals should be started well before any tools or applications are developed. Without programs that truly build and mature an analytically proficient security workforce, investigators and adjudicators risk becoming frozen in their ability to make difficult calls on difficult issues. The solution calls for training managers and working levels in structured analytic and decision-making techniques.

Even more importantly, it requires strong mentoring and support programs to ensure that analytic and decision-making capabilities improve over time. Harnessing the power of expanded data sets and innovative applications to highlight salient information will depend on the ability of the human workforce to make the calls and oversee the mitigations.

10. ENSURE CIVIL LIBERTIES AND PRIVACY OFFICES (CLPO) AND GENERAL COUNSEL REPRESENTATIVES ARE ACTIVE PARTICIPANTS IN CME PLANNING.

The CME concepts discussed in this paper conform to existing privacy laws and regulations, but implementing more frequent review of personnel and the potential use of social media and other Publicly Available Electronic Information (PAEI) requires close and active involvement by government CLPO and General Counsels. Government PAEI proof of concept evaluations in 2012 and 2013 involved CLPO and General Counsel representatives from the initial planning stages. The Federal Chief Information Officers (CIO) Council's Privacy Committee on PAEI issues published "Privacy Best Practices for Social Media" in July 2013, based on the work from these evaluations. Full discussion of civil liberties and privacy issues is essential to designing and implementing successful CME processes.

Interested in continuing the conversation?
Send your feedback to comments@insaonline.org, and
cite the name of this INSA White Paper in the subject line.

GLOSSARY

Several terms in this paper have different meanings for different users. The Subcommittee on Continuous Monitoring and Evaluation spent much time discussing various interpretations and determined the following definitions for the terms used in this paper:

CONTINUOUS MONITORING (CM): Committee on National Security Systems (CNSS) Instruction No. 4009 defines CM as "the process implemented to maintain a current security status for one or more information systems or the entire suite of information systems on which the operational mission of the enterprise depends. The process includes but is not limited to:

i. The development of a strategy to regularly evaluate selected information assurance (IA) controls/metrics;

ii. Recording and evaluating IA relevant events and the effectiveness of the enterprise in dealing with those events;

iii. Recording changes to IA controls, or changes that affect IA risks, and;

iv. Publishing the current security status to enable information sharing decisions involving the enterprise."

For the purposes of this paper, CM (also referred to as Insider Threat programs) is a highly automated, continuous process of detecting misuse of government information systems by authorized security clearance holders.

CONTINUOUS EVALUATION (CE): Executive Order 13467 defines CE as "reviewing the background of an individual who has been determined to be eligible for access to classified information (including additional or new checks of commercial databases, Government databases, and other information lawfully available to security officials) at any time during the period of eligibility to determine whether that individual continues to meet the requirements for eligibility for access to classified information."

For the purposes of this paper, CE is a continuous updating via automated records or database checks and review of a clearance holder's eligibility for access to classified information.

CONTINUOUS MONITORING and EVALUATION (CME): The Subcommittee has coined the term CME to emphasize that CM and CE are interconnected components that are essential to an enhanced, continuous Periodic Reinvestigation process. Their combination with other information—such as foreign travel and contacts, financial disclosures, polygraph results, and personnel actions—provides a more complete body of relevant information on which to base a periodic review of a clearance holder's eligibility for continued access to classified information.

ePERSONA: "ePersona" is an individual's online representation; this is independent of the person's use of or access to the internet. Online information is preserved and presented by any person or organization that keeps electronic records about individuals and their transactions, whether they be trips, purchases, credit, or employment. One's ePersona can be managed to some degree by fixing wrong information, challenging mistakes, and disputing erroneous transactions. This can become more difficult in the event that inappropriate and inflammatory material becomes part of one's ePersona or track record of online presence, activity, and behavior.

e-QIP: The "Electronic Questionnaire for Investigations Processing" is the online version of the Standard Form (SF)-86 used to record and upload personal information required for submission by someone being processed for access to sensitive and classified US Government information. The form formats the required information for immediate uploading into a database that requires no intermediate processing like the paper SF-86, form-fillable PDF, or Word version of the SF-86.

INITIAL BACKGROUND INVESTIGATION (IBI): The IBI is initiated when a government agency chooses to sponsor for the first time an individual's eligibility for access to classified information or eligibility to hold a sensitive position. The level of clearance can be for suitability or classified access like Secret, Top Secret, or higher. Each has its own requirements for gaining approval and includes some form of records checks and, at higher levels, interviews. Adjudication of the collected information allows for a determination to grant or deny the clearance.

PERIODIC REINVESTIGATION (PR): Once a person successfully completes an IBI, the PR is an updating investigation to reevaluate the clearance holder for continued clearance eligibility and access based on trustworthiness and responsibility for protecting classified information. In the case of a Top Secret or higher clearance, the PR is comprised of a combination of record checks, national agency checks, interviews, and a subject interview to cover the period of five years or since the date of the last investigation. For a Secret clearance, only the record and agency checks are conducted and for the period of 10 years; under a set of specified circumstances, the investigation may include a subject interview.

APPENDIX: The Future is Now: Assessing the "ePersona" in Background Investigations

The dynamic growth of online, internet-connected personal activity in the past ten years has been nothing short of astonishing. The rise and proliferation of "social media" tools and technologies has been a particular catalyst for that nearly exponential growth. A sampling of some of social media statistics is illuminating:

- 75.6 percent of the total US population (~245 million people) was estimated to be online by the end of 2012.[1]
- Over 66 percent of adults online in America are connected to one or more social media platforms.[2]
- 56 percent of Americans have a profile on a social networking site, and 22 percent of Americans use social networking sites several times per day.[3]
- 92 percent of American children have an online presence by the time they are two years old.[4]
- 87 percent of teens send text messages, and the average teen sends 3,339 texts per month.[5]
- 39 percent of Americans spend more time socializing online than face-to-face.[6]
- 85 percent of US adults share information online, 90 percent believe people share too much about themselves online, one-third are more comfortable sharing online than in person, and one in five admits to sharing false information online.[7]
- As of 2007, the average 21-year-old had: watched 20,000 hours (2.28 years) of TV; played 10,000 hours (1.14 years) of video games; talked 10,000 hours (1.14 years) on the phone; and sent or received 250,000 emails or instant messages (at 30 seconds per message, 2,083 hours, or .237 year), for a total of at least 4.797 years' worth of electronic/virtual activity.[8] *(Note: Assuming one-third of their 21 years would have been spent asleep, that means that over one-third of their remaining waking hours would have been spent performing such activity.)*
- There are over 1 billion people worldwide registered in virtual worlds (e.g., "World of Warcraft," "League of Legends," "Second Life") today, with the vast majority of users under the age of 25; tens of millions of those users live in China.[9]
- "Virtual Goods" revenues have grown from less than $1 billion in value in 2007 to roughly $14 billion in 2012;[10] "Second Life" actually issues quarterly "Virtual Economy Statistics" updates;[11] the "GDP" of Second Life grew from $64 million in 2006 to $567 million in 2009, about 25 percent of the entire US virtual goods market.[12]

The pace and level of activity on the internet is frenetic, as a snapshot from a single day in 2012 clearly illustrates: 294 billion emails are sent; 172 million people visit Facebook, spending more than 4.7 billion minutes on that site; 40 million visit Twitter; 22 million visit LinkedIn; 20 million visit Google+; 250 million photos are uploaded; 864,000 hours of video are uploaded to YouTube; more than 35 million apps are downloaded; and more iPhones are sold than people are born.[13] As staggering as those numbers appear, they continue to grow year on year—for example, Facebook had one million users in April of 2005; one hundred million in August 2008; and announced one billion users (of whom almost 175 million live in North America) as of October 2012.[14] Twitter, Google+, LinkedIn, Pinterest and other social media and gaming sites also report significant percentage growth in membership and usage.

These statistics are strong proof of what everyone intuitively knows—that the internet and all the tools and capabilities comprising it have become deep, ubiquitous and pervasive influences on the thoughts and behavior of a significant percentage of the human race. Moreover, that influence will continue to grow as the tools and technologies become more capable, economical (and hence available) and therefore attractive for greater human consumption and use.

The exponential growth in availability and use of social media has been a key factor in a concomitant exponential growth of digital data, which is referred to simply as "Big Data." According to technology estimates, as of 2012, about 2.5 exabytes (quintillion bytes) of data are created each day;[15] more data cross the internet every second today than were stored in the entire internet 20 years ago;[16] there will be 35 zetabytes (one zetabyte is 10 to the 21st, or a sextillion) of digital data[17] and 22 billion internet connected devices by 2020.[18] Other forecasts predict even greater digital growth: *Wired* magazine recently reported that the "Internet of Things" (IoT)—a global network of smart devices all linked together via the internet—will consist of one trillion devices, including both consumer and industrial sectors.[19] This proliferation of integrated data is affecting not just technology, but even our basic understandings of and insights into human behavior.

"This is a world where massive amounts of data and applied mathematics replace every other tool that might be brought to bear. Out with every theory of human behavior, from linguistics to sociology. Forget taxonomy, ontology, and psychology. Who knows why people do what they do? The point is they do it, and we can track and measure it with unprecedented fidelity. With enough data, the numbers speak for themselves."[20]

"WHAT THEY KNOW"[21]

Commercial technology companies have fully embraced this "brave new world" of Big Data, developing and deploying new and profoundly intrusive and ultimately insightful consumer-tracking technologies on a wide range of web sites. In fact, these efforts have created an entirely new "emerging industry of data-gatherers who are in effect establishing a new business model for the internet: one based on intensive surveillance of people *to sell data about, and predictions of, their interests and activities, in real time"* (emphasis added).[22] A number of studies and considerable research reveal the insight and clarity these new capabilities can achieve. MIT conducted a study of cell phone usage by a volunteer population living on campus, revealing "patterns of human behavior that could reveal how millions of people interact at home, work, and play…the data can predict with uncanny accuracy where people are likely to be at any given time in the future."[23] Among other findings in the study:

- With enough information about past movements, they could forecast someone's future whereabouts with 93.6 percent accuracy.
- Researchers were able to deduce that two people were talking about politics, even though the researchers didn't know the content of the conversation.
- Researchers were able to detect flu symptoms before the study subjects knew they were getting sick.[24]

Technology has evolved to the point that we now have the ability to adduce what people are not just doing but also thinking from their cell phone usage: *"Phones can know,"* said the director of MIT's Human Dynamics Lab, who helped pioneer the research. *"People can get this god's-eye view of human behavior* (emphasis added)."[25]

The research is not just academic; credit companies are deeply involved in developing new tools to predict credit scores and financial risk. The potential for understanding human behavior is so great that one executive from a credit reporting company stated, "We know what you are going to do tomorrow."[26] One new technology allows a company to know with a single click on its web site considerable details about the site visitor's education, family status, shopping patterns and home location, allowing the company to make decisions about whether people will be good customers even before they share the first bit of data about themselves. The CEO of [x+1] Inc., the company that created that technology, stated, "We never don't know anything about someone."[27]

The predictive value and utility of Big Data are clear, if not also ominous:

"[It] provides objective information about people's behavior. Not their beliefs or morals. Not what they would like their behavior to be. Not what they tell the world their behavior is, *but rather what it really is, unedited* (emphasis added). Scientists can tell an enormous amount about you with this data. Enormously more, actually than the best survey research, focus group, or doctor's interview—the highly subjective and incomplete tools we rely on today to understand behavior. With Big Data, current limitations on the interpretation of human behavior mostly go away. We can know whether you are the sort of person who will pay back loans. We can see if you're a good leader. We can tell if you're likely to get diabetes."[28]

To be sure, these new intrusive technologies enabled by "deep packet inspection"—reading and analyzing the countless packets of "ones and zeros" moving throughout the internet—allow for profiling and targeting internet users and will be controversial for, among other reasons, their impacts on personal privacy. But it will be very difficult to get the technology genie back in the bottle; one Internet Service Provider (ISP) executive stated, "The internet is becoming more and more a platform to deliver very targeted messages." Regarding deep packet inspection, "Everyone is going to get there. It's just a matter of time."[29]

USING SOCIAL MEDIA IN ANALYSIS AND DECISION-MAKING

Clearly, there is a growing convergence of new technologies and strong demand for better insights into personal behavior; this convergence has reportedly created demand in at least some quarters of the US Government for tools and capabilities to leverage these novel, potentially predictive capabilities. The Department of Homeland Security (DHS) has engaged the company Accenture in a one-year, $3 million program to conduct "biosurveillance" and attempt "to instantaneously spot public health trends among the massive amount of data that citizens share online daily."[30] The Defense Advanced Research Projects Agency (DARPA) has teamed with Carnegie Mellon University to create "an artificial intelligence system that can watch and predict what a person will 'likely' do in the future using specially programmed software designed to analyze various real-time video surveillance feeds. The system can automatically identify and notify officials if it recognizes that an action is not permitted, detecting what is [sic] described as anomalous behaviors."[31]

These new technologies have also found ready application in background investigations for hiring and access determinations. A person's online behavior is significantly revealing, and it is increasingly being accessed and studied for a range of personnel decisions, including college applications. "About a quarter of admissions officers at the nation's top 500 colleges have used websites such as Facebook and Google to vet applicants, according to an annual Kaplan Test Prep survey. Of those, more than one-third say they have found something that has hurt a student's chance of admission, up from 12 percent last year."[32]

The commercial sector is also producing new capabilities and products to enable thorough searches of online data resources for personnel vetting. LexisNexis has an entire line of business dedicated to employment screening and background checks, including a product called "Virtual ID," that leverages significant online searches to reveal relevant data about an individual's behavior and activity. The Social Intelligence Corp. (SIC) is another company that collects publicly available deep web content on subjects, consolidating all the unstructured data for review by company analysts. In particular, SIC can integrate specific adjudicative guidelines into its IT platform and filter the collected data through those standards for more rapid hiring or clearance determinations.

The background check and personnel analytic capabilities offered by these companies are not static or one-off; they are dynamic and continuous, offering the prospect for near real-time notification of new information that may have bearing on an individual's suitability for continued employment or access. Many companies, including investment banks, take advantage of those capabilities to continually monitor their employees long after the initial hiring decisions are made. This capability could be particularly relevant for US Government entities, which face huge backlogs in performing timely re-investigations of existing employees.

Interestingly, the private sector is also creating new tools for individuals to manage and monitor better their online and social media behaviors. For example, CyberPoint International has created an "app" called "Clearable™", which connects to Facebook users and analyzes their social media activity, such as postings, friends, fan pages, etc., and flags to the users any items that future employers and/or schools might find to be problematic. The flagged issues are based on the standards used in the government's Top Secret Security Clearance processes.[33]

LEGAL AND COMPLIANCE CONSIDERATIONS

The dramatic rise in social media and other behavior-related technologies has also created new concerns regarding how those technologies are used and their specific impacts on personal privacy. Anyone considering using internet-derived information for decision-making processes must ensure that all laws, regulations and privacy statutes are followed. The existence of such huge amounts of online data has, however, created a paradox for those entities choosing to use it for personnel decisions. If an organization decides to ignore the available information, it is not making its best effort and could be found liable for negligence if a problem arises subsequently that might have been avoidable or preventable based on the available information. On the other hand, if the organization using such data does not have an appropriate decision-making process in place, it may be exposed to legal action from the affected subject. Moreover, organizations may also face legal risks if they fail to make best efforts to ensure that the information used for decision-making is accurate and directly connected to the subject under investigation.

An understanding of the relevant regulations and privacy issues regarding using social media in personnel processes is best illustrated by a decision issued by the Federal Trade Commission (FTC). When Social Intelligence Corp. (SIC) was launched, the FTC began a non-public investigation into the company because it was the first to aggregate social media and publicly available online content to produce reports for employers to use in hiring processes. Upon completion of its investigation, the FTC determined that SIC and similar companies should be classified as "consumer reporting agencies" and must adhere to the rules under the Fair Credit Reporting Act (FCRA), which includes requirements for making best efforts to validate data.

The concept of "public data" is also subject to regular scrutiny. Defining what is "public" is a constant challenge that organizations face when attempting to define policies or procedures. There is a legal consensus that any data controlled by a user name and password would be considered "private" information, and any attempts to access and review that data would require explicit consent or a subpoena. Several states, including California and Maryland, have already passed legislation prohibiting asking individuals for their user names and passwords to gain access to the data on those sites. On the other

hand, there appears to be a consensus that web-based information that is not protected by user names and passwords is considered public data and therefore is accessible and reviewable by organizations making hiring or selection decisions. Such data would still be protected by other legal strictures (e.g., the First Amendment, Health Insurance Portability and Accountability Act Privacy Rule), but would otherwise be available for personnel decisions.

THE COUNTERINTELLIGENCE CHALLENGE

As discussed in this paper, the growth of social media and Big Data has combined to yield significant new insights into and understanding of human behavior, potentially to the point of predicting such behavior. Even if the Intelligence Community (IC) is reluctant to use such technology proactively to conduct background investigations and security determinations, it would be remiss if it did not exploit those capabilities for counterintelligence (CI) purposes. First, whether or not the IC chooses to use the new technologies, they will be commercially available to the rest of the world—hostile intelligence services will have access to those capabilities and can use them to target Americans with great precision and insight. The IC should not ignore the attendant CI vulnerabilities. Second, if the new technologies prove to be predictive of future behavior, there may be new tools and algorithms that could identify early-on problematic behaviors of greatest concern to the IC, including treason. It would be worth investing in a research and development effort to understand fully the CI applications for the new technologies.

OPPORTUNITIES FOR FUTURE IMPROVEMENTS

People are spending an increasing proportion of their life engaged in some form of online or virtual activity; the amount of accessible digital data is growing exponentially; it is increasingly possible to measure and monitor a person's online behavior with significant precision and fidelity, even to the point of accurately predicting future behavior; there are an increasing number of organizations that are using online data to make determinations about hiring and access; and there is an increasing understanding in the law regarding how online data may be used to make personnel-related decisions. And however accurate, insightful, and effective these technologies are today, they will likely get better with the relentless progression of Moore's Law.[34]

The US Government has, as noted, started to employ new tools and techniques to exploit social media for intelligence and security purposes. The US Intelligence Community must continue those efforts and embrace these capabilities, especially for use in making accurate, insightful, timely (and potentially predictive) evaluations about the suitability and reliability of their work force to hold positions requiring access to sensitive and classified information. Any background screening and evaluation process that omits a comprehensive review of an employee's "ePersona," or track record of online activity and behavior, will be incomplete in the new era and therefore represent a potential security and counterintelligence risk.

As an added benefit, any process using online capabilities to perform background screening will likely be faster, thereby potentially saving a significant amount of time and resources for both government and private sector firms doing government business. The opportunity to create a process for "continuous screening and monitoring" of subject employees could obviate much of the need and urgency of background "reinvestigations," which are subject to backlogs and time delays. In an era of resource limitations, saving money in the background screening process would allow other mission-focused priorities to be more fully funded.

The current environment of promising technologies emerging at the same time as a fiscally challenged federal government looks for efficiencies may well provide an opportunity to improve security while updating or eliminating costly, industrial age processes. Opportunities appear to exist for the Director of National Intelligence (DNI) and Director, Office of Personnel Management (OPM), as the security and suitability executive agents, in concert with the legislative branch to:

- Improve collaboration with the private sector to understand state-of-the-art online tools and technologies, define best practices, and discover the challenges and limitations of using such capabilities;
- Study and develop the parameters and norms of virtual behavior and the types of data that are relevant and appropriate for making determinations about suitability for access to classified information;
- Assess the counterintelligence implications of social media activities, including the significance of public posting of personal information, participation in virtual worlds, loss and accumulation of virtual wealth, virtual personal associations, and other relevant issues;
- Sponsor a legal review to establish clearly and transparently the rules, regulations and procedures necessary (e.g., comprehensive waivers, Fair Credit Reporting Act compliance, etc.) to enable rigorous use of online tools and techniques for background investigations and adjudicative decisions;
- Accelerate the application of online tools and techniques to "continuously evaluate" and assess eligibility of security clearance holders.

Interested in continuing the conversation?

Send your feedback to comments@insaonline.org, and cite the name of this INSA White Paper in the subject line.

ENDNOTES

[1] *www.b2bsocialmediaguide.com/2011/04/04/social-media-usage-statistics*

[2] *www.techtalkafrica.com/social-media-usage-statistics-for-2012-infographic.html/*

[3] *www.convinceandconvert.com/the-social-habit/11-shocking-new-social-media-statistics*

[4] *www.businesswire.com/news/home/20101006006722/en/digital-birth-online-world*

[5] *http://www.pewinternet.org/reports/2010/cell-phones-and-american-adults.aspx*

[6] *http://mashable.com/2010/10/14/nielsen-texting-stats*

[7] *Intel Survey on www.businesswire.com, May 9, 2012*

[8] *"Did You Know?" Karl Fisch, thefischbowl.blogspot.com, 2007*

[9] *KZero Worldswide (09-30-2010), www.kzero.co.uk*

[10] *Ibid*

[11] *www.secondlifeupdate.com*

[12] *Second Life," Wikipedia, October 2012*

[13] *http://thesocialskinny.com/100-social-media-mobile-and-interest-statistics-for-2012*

[14] *http://www.benphoster.com/facebook-user-growth-chart*

[15] *McAfee & Brynjolfsson, "Big Data: The Management Revolution," Harvard Business Review, October 2012*

[16] *Ibid*

[17] *IMS Research, www.imsresearch.com, 2010*

[18] *IDC Digital Universe Study, "Big Data is Here, Now What?" www.chucksblog.com, 2011*

[19] *Bill Wasik, "Welcome to the Programmable World," Wired, June 2013*

[20] *Chris Anderson, "The End of Theory: The Data Deluge Makes the Scientific Method Obsolete," Wired Magazine, June 24, 2008*

[21] *"What They Know" is the heading for a three year series of articles in the Wall Street Journal, 2010-2012, reporting on "a long-running investigation into the transformation of personal privacy in America." This paper quotes from several of those articles.*

[22] *Angwin & McGinty, "Sites Feed Personal Details to New Tracking Industry," Wall Street Journal, July 30, 2010*

[23] *Robert Lee Hotz, "The Really Smart Phone," Wall Street Journal, April 23, 2011*

[24] *Ibid*

[25] *Ibid*

[26] *Scott Thurm, "Next Frontier in Credit Scores: Predicting Personal Behavior," Wall Street Journal, October 27, 2011*

[27] *Steel & Angwin, "The Web's Cutting Edge, Anonymity in Name Only," Wall Street Journal, August 4, 2010*

[28] *Alex "Sandy" Pentland, "Predicting Customers' (Unedited) Behavior," Harvard Business Review Blog Network, September 19, 2012*

[29] *Stecklow & Sonne, "Shunned Profiling Technology on the Verge of Comeback," Wall Street Journal, November 24, 2010*

[30] *Aliya Sternstein, "DHS tries monitoring of social media for signs of biological attacks," NextGov, November 15, 2012*

[31] *"DARPA seeking surveillance technology to predict future behavior," HS News Wire, November 24, 2012*

[32] *Belkin & Porter, "Web Profiles Haunt Students," Wall Street Journal, October 4, 2012*

[33] *See www.clearable.us/portal for more information*

[34] *Posited by Gordon Moore in 1965, Moore's Law predicts that the numbers of transistors on an integrated circuit will double every 24 months at constant cost. The "Law" has been applied to other areas of digital technology, including processing speeds, memory capacity, camera pixels, etc. The technologies underlying social media and Big Data will, therefore, continue to grow exponentially in the future.*

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

ABOUT THIS INSA SPRC WHITE PAPER

The INSA Security Policy Reform Council (SPRC) established in April 2013 the Subcommittee on Continuous Monitoring and Evaluation, along with three other subcommittees on security metrics, reciprocity, and technologies, to review the information and technology that could enhance the security clearance process. Specifically, it asked if and how known commercial technology used as part of "continuous monitoring and evaluation" (CME) could enhance the periodic reinvestigation (PR). Once determining it could, the Subcommittee focused on ways to enable the current PR process to be more timely, effective, and cost-efficient and to improve the inconsistent availability and reciprocity of personnel security clearance data.

This white paper documents the subcommittee's findings, building on INSA's previous report, "Next Steps for Security Reform," published in December 2011 and the point paper, "The Future is Now: Assessing the 'ePersona' in Background Investigations," presented in March 2013 at the INSA Security and Acquisition Symposium (The point paper is included as an Appendix). The Council's recommendations are geared toward demonstrating how technology can be used to balance and leverage CME with the "traditional" PR. The CME discussed in this paper can apply equally to the Initial Background Investigation (IBI) portion of the security clearance process, but the focus of this study is on remedies for the challenges facing the current periodic reinvestigation process.

ABOUT INSA

INSA is the premier intelligence and national security organization that brings together the public, private and academic sectors to collaborate on the most challenging policy issues and solutions.

As a non-profit, non-partisan, public-private organization, INSA's ultimate goal is to promote and recognize the highest standards within the national security and intelligence communities.

INSA has over 150 corporate members and several hundred individual members who are leaders and senior executives throughout government, the private sector and academia.

To learn more about INSA visit www.insaonline.org.

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

BUILDING A STRONGER INTELLIGENCE COMMUNITY

901 North Stuart Street, Suite 205, Arlington, VA 22203
(703) 224-4672 | www.insaonline.org