AFRL-RI-RS-TR-2018-260

IMPACT PORTAL

BLACKFIRE TECHNOLOGY, INC.

OCTOBER 2018

FINAL TECHNICAL REPORT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

STINFO COPY

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE

■ **AIR FORCE MATERIEL COMMAND** ■ **UNITED STATES AIR FORCE** ■ **ROME, NY 13441**

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09. This report is available to the general public, including foreign nations. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RI-RS-TR-2018-260 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE CHIEF ENGINEER:

/ S /
ROBERT KAMINSKI
Work Unit Manager

/ S /
JAMES PERRETTA
Acting Deputy Chief, Information Exploitation & Operations Division
Information Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
OCTOBER 2018	FINAL TECHNICAL REPORT	JUL 2017 – JUL 2018

4. TITLE AND SUBTITLE

IMPACT PORTAL

5a. CONTRACT NUMBER
FA8750-17-C-0173

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
NA

6. AUTHOR(S)

Dustin Henson

5d. PROJECT NUMBER
DHSB

5e. TASK NUMBER
LA

5f. WORK UNIT NUMBER
CK

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Blackfire Technology Inc.
4896 North Edie Drive
Kingman, AZ 86409

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Research Laboratory/RIG
525 Brooks Road
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/RI

11. SPONSOR/MONITOR'S REPORT NUMBER
AFRL-RI-RS-TR-2018-260

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited. This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The IMPACT Portal project was created to serve as a secure platform to facilitate the responsible sharing of research data between Researchers involved in cybersecurity. The goal of the project is to provide a discovery system and efficient data sharing process through which members of the IMPACT community can get access to existing data to accelerate their design, production, and evaluation of cybersecurity solutions as well as further research. IMPACT acts as a bridge between Providers who produce data relevant to the field and those who have a use for the data.

15. SUBJECT TERMS

Cyberspace data collection, cyberspace data storage, cyberspace storage retrieval

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			**ROBERT KAMINSKI**
U	U	U	UU	13	19b. TELEPHONE NUMBER (*Include area code*) **NA**

TABLE OF CONTENTS

Section **Page**

1.0 SUMMARY

The following report contains information concerning the involvement of Blackfire Technology, Inc. (Blackfire) in the IMPACT Portal project during the July 2017 - July 2018 contract year. Included in the report is information about the many achievements of Blackfire during the contract. The report also details some of the challenges encountered by the team and the steps taken to mitigate such challenges. Finally, we present our conclusions regarding the contract year and our hopes for the future of the IMPACT Portal project.

2.0 INTRODUCTION

The IMPACT Portal project was created to serve as a secure platform to facilitate the responsible sharing of research data between Researchers involved in cybersecurity. The goal of the project is to provide a discovery system and efficient data sharing process through which members of the IMPACT community can get access to existing data to accelerate their design, production, and evaluation of cybersecurity solutions as well as further research. IMPACT acts as a bridge between Providers who produce data relevant to the field and those who have a use for the data.

Blackfire has been the team behind the IMPACT Portal technology from July 2017 through July 2018. As such, it has been our responsibility to ensure the IMPACT Portal remains in good working order so that approved Researchers can access and utilize the data they need and so that Providers can continue to supply datasets and tools to the IMPACT community.

In addition to maintaining the IMPACT Portal, Blackfire has sought to improve the Portal experience for researchers, providers and administrators. Our goal has been to make the Portal easier to use, allowing for greater productivity. We have strived to make functionality and efficiency enhancements across the project, including Portal design and in the procedures that affect its use, such as the approval process.

3.0 METHODS, ASSUMPTIONS, AND PROCEDURES

3.1 Methodology

Initially, the Blackfire technical team followed a lightweight, but industry standard process that involved creating a design document prior to starting development. However, this proved ineffective in the IMPACT environment. Subject Matter Experts (SMEs) were not available to give the input needed to properly design new features and were not available to review the completed designs in a timely fashion. This lead to repeated instances of rework, despite having spent significant time on designs. As a result, project management and the Blackfire team agreed to move to an "agile development" style that consisted of light design followed by multiple iterations of development and refinement. This process has proven effective in the IMPACT environment and continues today.

Throughout the project, the IMPACT team followed the procedures detailed in the following documents, which were previously submitted:

- IMPACT Coordinating Center (ICC) Administrators: IMPACT Portal - ICC SOP Manual of Operations.
- Regression Testing: IMPACT Portal - Test Scripts.
- Disaster Recovery: IMPACT Portal - Disaster Recovery Process.
- Release Process: IMPACT Portal - Setup & Configuration Guide.

3.2 Work Completed

One of the initial tasks Blackfire completed was to revise the agreements and contracts that Researchers must accept to receive access to data. This included both the IMPACT specific agreements and the versions that appear on the Portal for public use. The agreements with Providers were also updated to give the Portal team greater flexibility in sharing data. For example, the ICC was allowed to provide researchers with year-long umbrella contracts for receiving access to all Restricted data, instead of needing individual contracts for each dataset.

Blackfire also expanded the Portal's catalog of records to include "Tools" and "External" records. The rollout was successful, and users immediately began adding records to the catalog without the assistance of the ICC team. This was a great benefit for the community as tools for processing data became available. And, valuable data available outside of the IMPACT processes could also be found while searching the IMPACT catalog.

Throughout the course of the contract, Blackfire implemented several changes. Some of the changes included:

- Two DOI enhancements were completed, allowing providers to add global DOI locators to both Datasets in the Catalog and the Research Paper list with IMPACT.
- The bulk XML upload system was enhanced to send an automated email to the Admins and the Provider representative when datasets are updated through bulk XML upload.
- New dataset category codes were implemented, and all old datasets were changed from their old codes to the new ones.
- A new production server was built with increased storage, an upgraded operating system, and upgraded software.

- A new test server was built after Amazon retired the hardware used by the previous test server. As part of this process, Blackfire formalized a disaster recovery process, which was used to create a new test server.
- Data Use Terms were made part of the dataset records, allowing providers to have different terms for each restricted dataset and also to update them directly through the Dataset Edit screen or through bulk XML upload.
- Email services were transferred to a new provider, allowing for greater availability and privacy.
- The search system was enhanced to improve the speed and logic, including bringing on board an advanced search provider, Inferlink.
- The dataset ranking system was enhanced to change the way search results were ordered and to make more information about ranking available to Researchers.
- Numerous aesthetic changes were made to the IMPACT Portal that also make it easier for users to navigate.

In addition to changes to the system, Blackfire also created several documents that detail IMPACT processes and procedures. Some of the documents created are:

- ICC Manual of Operations.
- Server Infrastructure.
- Database ER Diagram.
- Test Scripts for Regression Testing.
- Setup and Configuration Guide.
- New Provider Quickstart Guide.
- Disaster Recovery.
- Portal Design Documents.
- User Guide.

3.3 Challenges Encountered

The contract year was not without its challenges. During the year, IMPACT administration and the Blackfire team dealt with problems of various natures, including technical problems, IMPACT team problems, and user problems.

3.3.1 Technical Problems. In today's world, it is not uncommon for Internet-based platforms like IMPACT to be subjected to hacking attempts. We encountered several such attempts during the contract year.

One occurred in 2017 when a sophisticated and coordinated effort was made to flood the IMPACT system with fraudulent user requests. We refer to this as the "Bot Attack" as it was all computer-generated content. These requests came from computers all over the world and seemed to contain real data.

Had the account approval process been automated, a large number of these would have succeeded. However, members of the administration team looking at the requests quickly spotted patterns in how the names were generated. They also saw that the addresses were comprised of

real location elements put together in nonsensical ways and that the text in free text fields was gibberish.

There have also been repeated instances of a sophisticated Russian search engine bombarding the IMPACT Portal site with millions of requests. This resulted in search performance issues and system instability. Initially, the problem presented as the hard drive filling up. To fix this, Blackfire performed a regular cleanup of old working files to clear space. Normally, this is done once every couple of months. However, by the weekend, the hard drive was full again. On Monday, the drives were at a critical level. With the other working files already cleaned up, it became clear that the issues were due to abnormally large log files from user traffic.

Upon discovering that the disk space issue was a symptom of a larger problem, our team began investigating. We discovered that the search page was being hit 3-4 times per second by a Russian search engine called Yandex.

Blackfire made several changes to mitigate these hacking attempts and denial of service type attacks as well as future attempts. First, the Portal's Security Proxy was upgraded with additional security rules. Direct hacking attempts need to penetrate these layers before reaching the Portal application. In addition, the proxy is able to monitor incoming and outgoing user communication.

The dynamic security module Mod Security looks for traffic and usage patterns that could indicate hacking attempts. When it spots suspicious traffic, that user's access is shut down for a period of time. As updates are made to the Portal, Mod Security's rules takes regular maintenance to ensure that valid traffic is not flagged. The second change was to update Mod Security's rules to detect several indicators that communication was coming from Yandex and to block that traffic.

In addition, firewall rules were put in place to block access to computers known to cause issues. For example, the Russian search engine was blocked by a combination of Mod Security rules and firewall rules.

Finally, we added Google's Capcha to the Account Request page to validate that the user is a human and not a bot. This effectively blocked the bogus account requests from the Bot Attack.

3.3.2 IMPACT Team Problems. Partner organizations in each of the DHS approved countries review and process foreign account requests. These individuals are called International Account Coordinators (IAC). Staffing turnover and the low priority of IMPACT at some of these organizations has led to account requests not being processed in a timely manner. In some cases, account requests have gone unprocessed for months. The Israel IAC position seems to be vacant. To mitigate the problem, Project Management has directed the ICC to process these requests until a new Israel IAC is in place. In other cases, Project Management is working with those IACs through Department of Homeland Security (DHS) channels.

3.3.3 User Problems. Some problems encountered by Blackfire over the course of the contract have to do with problems that stem from the user's side. One problem we have encountered is attempts by users to deceive the ICC. The ICC Admin Team has run across numerous instances

of dishonest researchers or others from non-DHS approved countries attempting to receive access to information by providing false information. ICC reviews each individual request and works diligently to deny requests from people and organizations who provide false information.

In other cases, valid users have difficulty getting Memorandums of Agreement (MOAs) through their legal departments. Researchers are required to provide a signed MOA to receive access to restricted data. Previously, a new MOA was needed for each request. The policy has now changed to allow MOAs to be applied to future requests for one year, making information more accessible to Researchers. However, many Researchers still struggle to have that MOA approved by their legal departments.

Another problem we have encountered is the difficulty users have finding the IMPACT portal on the Internet. For certain search terms, IMPACT is hard to find using search engines. Immediately after the Portal was optimized for search engines using search engine optimization (SEO) techniques, the IMPACT Portal and its content was rated highly by Google. However, it quickly fell in the search results.

For Google and other major search systems, ranking in search results works by counting external links and weighting them by the importance of the site the link is on. So, a link in the New York Times elevates your score much more than a link that appears in John Doe's personal blog. For this reason, the primary way to raise IMPACT in the search results and help Researchers find it is to have external sites link back to IMPACT.

Unfortunately, publicizing IMPACT is beyond the scope of what the technical team can do. We recommend that Project Management and the Providers publicize IMPACT through Facebook posts, press releases, and blog forums. All attempts to publicize the Portal should include a link back to one of the IMPACT Portal pages.

4.0 RESULTS AND DISCUSSION

Overall, we believe Blackfire and the IMPACT project had a very successful year. Through the hard work of our team, the ICC Admin approval times have dramatically improved from before we took over. Requests are now approved on the first business day as opposed to a week or more. Overall approval times are also down considerably. Providers are able to more quickly approve Quasi-Restricted and Restricted dataset requests because of improved Portal approval screen features and automated reminder emails. So, despite challenges outside of the technical team's control, such as the IAC issues and user response times for MOA signatures, the average user's response time has improved considerably.

The Portal has also become more user-friendly during the course of the contract. The enhanced search system makes finding appropriate records easier and faster than ever. The approval process has been streamlined, allowing Researchers to begin using datasets more quickly than in previous years. And, navigating the system is also easier because of improvements to its appearance. All of these things allow Researchers, Providers, and Administrators to be more productive.

Though the IMPACT Portal has become easier to use, we still feel that prospective users are having trouble finding IMPACT. Unfortunately, IMPACT has not been widely publicized on the Internet. We strongly believe that increasing the publicity would bring more users into the IMPACT community. As demonstrated through SEO changes made to the site and through an uptick in account requests after conference presentations and publications, IMPACT needs to be publicized both through the various social media outlets and through direct contact.

5.0 CONCLUSIONS

The Blackfire team has been honored to be a part of the IMPACT community. We believe that our many accomplishments during the course of the contract have greatly improved the system, both in its technical aspects and in the administrative procedures. Just a few of our accomplishments during the contract are:

- Better search engine speed and results.
- Improved user navigation.
- Enhanced catalog features.
- Improved response times.
- Time-saving automation of certain processes, such as reminder emails.
- Improved approval processes, including updated agreements and use of MOAs for all restricted and quasi-restricted requests for one year.
- Creation of documents that outline process and procedures for the administrative team and users.

Blackfire would welcome the opportunity to continue our involvement with the IMPACT Portal project. We hope to see the community grow through additional publicizing of the project and its many advantages for Researchers. We believe that there are many opportunities for continued improvement of the project and would be honored to be a port of its future.

LIST OF SYMBOLS, ABBREVIATIONS, AND ACRONYMS

DHS	Department of Homeland Security
IAC	international account coordinators
ICC	IMPACT coordinating center
MOAs	memorandums of agreement
SEO	search engine optimization
SMEs	subject matter experts