2131 PALOMAR AIRPORT RD., STE. 239
CARLSBAD, CA 92011
800.240.3280
WWW.911EDA.COM

System Security Plan (SSP) for Controlled Unclassified Information (CUI)

911EDA, Carlsbad CA 92011

Version 2.1 | Date of Last Revision: November 22, 2023

Document Control

Version History

Version	Date	Description of Changes	Author(s)
1.0	02/17/2019	Initial creation of the System Security Plan (SSP).	SSP Team
1.1	06/15/2019	Updated to include additional encryption protocols.	SSP Team
1.2	12/08/2019	Revised incident response procedures and added new training modules.	SSP Team
1.3	05/23/2020	Enhanced access control measures and updated malware protection solutions.	SSP Team
1.4	11/14/2020	Introduction of continuous monitoring practices.	SSP Team
1.5	04/07/2021	Adjustments to the data handling policy for clarity and compliance.	SSP Team
1.6	08/19/2021	Revision of security awareness training content.	SSP Team
1.7	12/01/2021	Incorporation of feedback mechanism for continuous improvement.	SSP Team
2.0	06/05/2023	Major update to align with the latest NIST SP 800-171 revision.	SSP Team
2.1	11/22/2023	Minor updates to risk assessment procedures and training curriculum.	SSP Team

Approval

The current version of this System Security Plan (SSP), Version 2.1, dated November 22, 2023, has been reviewed and is hereby approved by:

- **Ryan O'Connor**, President

Distribution List

This System Security Plan (SSP) is distributed to and must be accessible by all employees of 911EDA. All employees are required to familiarize themselves with the security policies and procedures contained within this document and to adhere to the principles and guidelines outlined herein to ensure the protection of Controlled Unclassified Information (CUI).

Section 1: Document Overview

1.1 Purpose The purpose of this System Security Plan (SSP) is to outline the security measures implemented by 911EDA to protect Controlled Unclassified Information (CUI) in accordance with the requirements outlined in NIST Special Publication 800-171. This document provides an overview of the security controls, policies, procedures, and responsibilities related to safeguarding CUI within our organization.

1.2 Scope This SSP applies to all information systems, networks, and resources owned, operated, or utilized by 911EDA that store, process, or transmit CUI. It encompasses both internal systems and external systems operated on behalf of 911EDA. All employees, contractors, and third-party entities with access to CUI are subject to the provisions outlined in this plan.

1.3 Objectives The objectives of this System Security Plan (SSP) underscore our comprehensive approach to securing Controlled Unclassified Information (CUI) within 911EDA. Our commitment extends beyond compliance, aiming to foster a resilient and aware organizational culture, adept at navigating the evolving cybersecurity landscape. The revised objectives include:

- **Ensure Compliance with NIST SP 800-171 Requirements**: To meet the stringent standards set forth by the National Institute of Standards and Technology (NIST) Special Publication 800-171, guaranteeing that our security practices robustly protect CUI and align with federal expectations.
- **Adhere to DFARS 252.204-7012 Requirements**: To diligently comply with the Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012, affirming our dedication to securing defense-related information and contributing to the collective defense cybersecurity posture.
- **Safeguard the Confidentiality, Integrity, and Availability of CUI**: To implement rigorous security measures that protect CUI against unauthorized access, disclosure, alteration, or destruction, thus ensuring the information's reliability and availability to support national security and our clients' missions.
- **Establish Clear Security Policies, Procedures, and Controls**: To mitigate risks associated with CUI handling through comprehensive, understandable, and actionable security guidelines that govern our operations and employee conduct.
- **Promote a Culture of Security Awareness and Accountability**: To cultivate an environment where security is a shared responsibility, encouraging all employees and stakeholders to actively participate in protecting CUI and being vigilant about potential threats.
- **Provide a Framework for Continuous Monitoring, Assessment, and Improvement**: To adopt a proactive stance on security by continuously evaluating the effectiveness of our security measures, embracing technological advancements, and adapting to emerging threats and regulatory changes.
- **Enhance Collaboration with the Department of Defense (DoD) and Defense Contractors**: To strengthen our partnerships within the defense sector, sharing insights and adopting best practices to contribute to a unified and secure defense industrial base.

Through these objectives, 911EDA commits to maintaining the highest security standards for CUI, reflecting our role as a trusted partner in the defense supply chain and our dedication to national security.

1.4 Document Structure This SSP is structured as follows:

- Section 1: Document Overview
- Section 2: System Description
- Section 3: System Security Controls
- Section 4: Control Implementation
- Section 5: Security Policies and Procedures
- Section 6: Risk Assessment and Management
- Section 7: Incident Response Plan
- Section 8: Security Awareness and Training
- Section 9: Continuous Monitoring and Assessment
- Section 10: Plan Maintenance and Updates
- Section 11: References and Appendices

Each section provides detailed information on specific aspects of our CUI protection program, including descriptions, implementation details, and associated documentation.

Section 2: System Description

2.1 Overview of System Architecture

At 911EDA, our centralized system architecture is meticulously designed to manage and protect Controlled Unclassified Information (CUI) throughout its entire lifecycle, from the initial acquisition to the final transfer to our clients. This architecture is pivotal in ensuring the security and integrity of CUI, facilitating our commitment to safeguarding sensitive information against unauthorized access, disclosure, modification, or destruction.

2.2 Detailed Architecture Components

- **Central Server**: The heart of our infrastructure, the central server, is tasked with the initial reception and processing of CUI from external sources. Equipped with state-of-the-art security measures, this server ensures the confidentiality, integrity, and availability of the information it processes. Access is stringently controlled and limited to personnel with explicit authorization, thus fortifying our defense against unauthorized access or manipulation.
- **Offline Machines**: Following reception, CUI is transitioned to offline machines. These systems are deliberately segregated from external networks, including the Internet, creating an air-gapped environment that significantly diminishes the risk of external threats. These machines are dedicated to the in-depth processing and analysis of CUI, employing robust security measures like endpoint protection, encryption, and regular security updates to enhance resilience against potential threats.
- **Secure Transfer to Customers**: Upon completion of processing, CUI is securely transferred back to the central server in preparation for customer distribution. This transfer process adheres to stringent protocols, employing data encryption and secure file transfer methods to ensure the

utmost protection of CUI during transit. Access to customer data on the central server is rigorously controlled, with measures in place to prevent any unauthorized access or disclosure.

2.3 Visualization and Documentation

Detailed network diagrams and system specifications are maintained to provide a comprehensive understanding of our system architecture. These documents offer insight into the central server configuration, the setup of offline machines, and the data transfer procedures, ensuring transparency and clarity in our CUI handling processes.

2.4 Commitment to Security

Our system architecture is designed with a deep commitment to security at its core. By maintaining detailed documentation and adhering to strict security protocols, we ensure the safeguarding of Controlled Unclassified Information, reflecting our dedication to protecting the sensitive data entrusted to us by our clients and partners.

Section 3: System Security Controls

In our pursuit of effectively protecting Controlled Unclassified Information (CUI), we implement a robust suite of system security controls. These measures are thoughtfully selected and rigorously enforced to safeguard against unauthorized access, disclosure, modification, or destruction of CUI. Below, we detail the rationale and implementation of key security controls within our system.

3.1 Access Control

- **Objective**: To ensure that access to CUI is strictly granted based on the principle of least privilege and need-to-know basis.
- **Justification**: Limiting access minimizes the risk of accidental or malicious data breaches, ensuring that only authorized personnel can interact with sensitive information.
- **Implementation**: We deploy role-based access controls (RBAC) and access control lists (ACLs) to enforce our access control policies. User roles are defined based on job responsibilities, with permissions tailored to the minimum necessary for each role. Access reviews are conducted regularly to ensure alignment with current roles and responsibilities, and multi-factor authentication (MFA) is mandatory for all users accessing systems containing CUI.

3.2 Data Encryption

- **Objective**: To protect the confidentiality and integrity of CUI during storage and transmission.
- **Justification**: Encryption acts as a last line of defense, rendering data unreadable to unauthorized individuals even in the event of a security breach.
- **Implementation**: We utilize Advanced Encryption Standard (AES) algorithms for encrypting data at rest and in transit. Encryption keys are managed securely, with strict key lifecycle management practices, including regular rotation and secure storage. This ensures that even if data is intercepted, it remains protected against unauthorized access.

3.3 Network Security

- **Objective**: To secure the network infrastructure against unauthorized access, intrusions, and other threats.
- **Justification**: Robust network security is critical to preventing attackers from accessing systems that store, process, or transmit CUI.
- **Implementation**: Our network security architecture includes segmentation to isolate sensitive data, firewalls to control incoming and outgoing traffic, and Intrusion Detection and Prevention Systems (IDPS) to monitor for suspicious activity. These controls work in concert to create a defense-in-depth strategy that protects against a wide range of cyber threats.

3.4 Malware Protection

- **Objective**: To prevent, detect, and remove malware from all systems within the organization.
- **Justification**: Malware can compromise system integrity, confidentiality, and availability. Proactive malware protection is essential to maintain the security of CUI.
- **Implementation**: Endpoint protection solutions are installed on all devices, with regular updates and scans to ensure effectiveness against new and evolving malware threats. Email and web content filtering solutions are employed to prevent phishing attacks and access to malicious websites, further reducing the risk of malware infection.

Section 4: Control Implementation

4.1 Access Control Implementation Access control policies and procedures are enforced through the use of role-based access controls (RBAC) and access control lists (ACLs). User accounts are regularly reviewed and updated to align with organizational roles and responsibilities. Access logs are maintained to track user activity and identify unauthorized access attempts.

4.2 Data Encryption Implementation Data encryption uses industry-standard cryptographic algorithms such as AES (Advanced Encryption Standard). Encryption keys are generated, stored, and managed securely to prevent unauthorized access. Key rotation and critical management practices are followed to maintain the confidentiality and integrity of encrypted data.

4.3 Network Security Implementation Network security measures are implemented at the perimeter and internal network levels to protect against unauthorized access and data breaches. Firewalls are configured to enforce access control policies and filter network traffic based on predefined rules. Intrusion detection/prevention systems (IDPS) are deployed to monitor network activity and detect potential security incidents in real time.

4.4 Malware Protection Implementation Endpoint protection solutions are deployed on all endpoints, including servers, workstations, and mobile devices, to detect and prevent malware infections. Antivirus software is configured to perform regular scans and updates to detect and remove malicious software.

Email filtering and web content filtering solutions are integrated to block phishing attempts and malicious websites.

Section 5: Security Policies and Procedures

Our commitment to safeguarding Controlled Unclassified Information (CUI) is reflected in the comprehensive suite of security policies and procedures we have developed. These policies and procedures are designed to ensure that every team member understands their role in protecting sensitive information and is equipped with the knowledge to do so effectively.

5.1 Enhanced Password Policy

- **Objective**: To strengthen user account security through robust password practices.
- **Justification**: Passwords are a critical line of defense against unauthorized access. Enhancing password policies ensures that this defense is as strong as possible.
- **Implementation**: Our enhanced password policy mandates the use of password managers for generating and storing complex passwords. We encourage using passphrases, which are longer and more complex than traditional passwords yet easier for users to remember. Passwords must meet minimum complexity requirements, including length, character variety, and uniqueness. Regular password changes are enforced, and users are educated on the importance of not reusing passwords across different systems or sharing them with others.

5.2 Data Handling and Protection Policy

- **Objective**: To outline the correct procedures for handling, storing, and transmitting CUI, ensuring its protection at all times.
- **Justification**: Proper data handling minimizes the risk of accidental or deliberate data breaches, protecting our clients and our organization.
- **Implementation**: The Data Handling and Protection Policy details specific dos and don'ts for managing CUI:
    - **Dos**:
        - Always use encrypted channels to transmit CUI.
        - Store CUI in designated secure areas with controlled access.
        - Follow the clean desk policy, ensuring sensitive information is not left unattended.
    - **Don'ts**:
        - Avoid using unapproved devices or applications to access or process CUI.
        - Do not share CUI with unauthorized individuals, even within the organization.
        - Refrain from transmitting CUI over unsecured networks.
        -

5.3 Incident Response Policy

- **Objective**: To establish a clear and effective process for responding to CUI security incidents.

- **Justification**: A structured response to incidents minimizes potential damage and facilitates a swift return to normal operations.

- **Implementation**: Our Incident Response Policy outlines the steps to be taken in the event of a security incident:

1. **Detection and Reporting**: Employees are trained to recognize and promptly report security incidents.
2. **Assessment**: The incident response team assesses the scope and impact of the incident.
3. **Containment and Eradication**: Steps are taken to contain the incident and eliminate the threat.
4. **Recovery**: Affected systems are restored and returned to normal operation.
5. **Post-Incident Analysis**: The incident is reviewed to improve future response efforts.

Training and awareness activities ensure all employees understand their roles in the incident response process, and drills are conducted regularly to test and refine our response capabilities.

Section 6: Risk Assessment and Management

6.1 Risk Assessment Process 911EDA conducts regular risk assessments to identify, analyze, and prioritize risks to CUI within the organization. Risk assessments consider factors such as threat actors, vulnerabilities, and potential impacts on business operations. Risk treatment strategies are developed to mitigate identified risks and reduce their likelihood and impact.

6.2 Risk Management Plan A risk management plan documents the organization's approach to managing risks associated with CUI handling. It includes risk assessment methodologies, risk acceptance criteria, and risk treatment plans. Risk management activities are integrated into the organization's overall cybersecurity program and are subject to regular review and update.

Section 7: Incident Response Plan

Our Incident Response Plan (IRP) is meticulously crafted to ensure a coordinated and effective response to security incidents that could impact the Controlled Unclassified Information (CUI) we manage. The IRP is designed to minimize the impact of incidents through swift action and to restore the integrity of our systems as quickly as possible.

7.1 Incident Response Team

- **Composition**: The Incident Response Team (IRT) comprises members from various departments, including IT security, legal, and communications, each bringing specialized knowledge and skills. A designated Incident Response Coordinator leads this team.

- **Training and Preparedness**: Team members receive ongoing training in incident response tactics and procedures. Regular simulation exercises are conducted to ensure the team's readiness and effectiveness in handling real incidents.

7.2 Incident Detection and Reporting

- **Mechanisms**: We employ a combination of automated systems and employee vigilance to detect potential security incidents. Our tools include intrusion detection systems, security event log monitoring, and anomaly detection algorithms.

- **Reporting Procedures**: All employees are trained to recognize signs of security incidents and are provided with clear instructions for reporting these observations. A dedicated incident reporting hotline and email address are maintained to facilitate prompt reporting.

7.3 Incident Assessment and Classification

Upon receiving a report of a potential incident, the IRT conducts an initial assessment to classify the incident based on severity and impact. This classification guides the response strategy and prioritization of response actions.

7.4 Incident Response Phases

1. **Preparation**: Beyond training and simulations, preparation includes maintaining up-to-date response tools and access to critical resources.
2. **Identification**: Quick and accurate identification of an incident's nature and scope is critical for effective containment and eradication.
3. **Containment**: Short-term containment actions are taken to prevent further damage, followed by long-term containment to ensure system integrity during recovery.
4. **Eradication**: The incident's root cause is addressed, and affected systems are cleaned to remove any traces of the threat.
5. **Recovery**: Systems are restored and returned to normal operations with monitoring in place to ensure they are not compromised.
6. **Lessons Learned**: After an incident, the team reviews to identify improvements to processes, training, and tools.

7.5 Continuous Improvement

Feedback from incident post-mortems is integrated into the IRP to enhance responsiveness and effectiveness. This process ensures that our incident response strategies evolve in line with emerging threats.

Section 8: Security Awareness and Training

A cornerstone of our defense strategy is the ongoing security awareness and training provided to all employees. This program is designed to equip every team member with the knowledge and tools they need to contribute to the security of CUI.

8.1 Security Awareness Program

- **Objective**: To foster a culture of security awareness where all employees understand their role in protecting CUI and are equipped to do so effectively.

- **Activities**: Our program includes regular security briefings, newsletters, and alerts about current cyber threats. Interactive learning experiences, such as phishing simulations, reinforce the practical application of security principles.

8.2 Tailored Training Curriculum

- **Customized Content**: Recognizing the diverse roles within our organization, we tailor our training content to address the specific security concerns of different departments. For example, our IT staff receive in-depth training on technical security controls, while administrative personnel are trained on data handling practices and phishing identification.

- **Continuous Learning**: Security training is not a one-time event but an ongoing process. Employees undergo annual refresher courses, and new hires receive security orientation sessions. Our curriculum is regularly updated to reflect the latest security trends and best practices.

- **Empowerment through Education**: By empowering our employees with knowledge and awareness, we enhance our collective ability to safeguard CUI against evolving threats. Our commitment to continuous education underscores our dedication to maintaining the highest information security standards.

Section 9: Continuous Monitoring and Assessment

9.1 Continuous Monitoring 911EDA implements continuous monitoring mechanisms to assess the effectiveness of security controls and detect potential security threats in real time. Monitoring tools and technologies are deployed to collect and analyze security-related data from various sources within the organization's IT environment.

9.2 Security Assessment Periodic security assessments are conducted to evaluate the organization's compliance with security policies, procedures, and regulatory requirements. Security assessments may include vulnerability scans, penetration tests, and compliance audits conducted by internal or external auditors.

Section 10: Plan Maintenance and Updates

To ensure the continued relevance and effectiveness of our System Security Plan (SSP) for the protection of Controlled Unclassified Information (CUI), we are committed to a rigorous program of regular reviews, updates, and continuous improvement. This process ensures that our security posture remains robust against evolving threats and aligns with best practices and compliance requirements.

10.1 Regular Review and Revision

- **Scheduled Reviews**: The SSP is formally reviewed and assessed for comprehensiveness and effectiveness at least annually. These reviews are timed to align with significant changes in our technology infrastructure, major updates to relevant regulations, or in response to lessons learned from security incidents.

- **Ad Hoc Updates**: In addition to scheduled reviews, the SSP is updated on an as-needed basis to respond to immediate changes in the threat landscape, emerging technology, or organizational structure.

10.2 Incorporation of Stakeholder Feedback

- **Feedback Mechanism**: We encourage feedback on the SSP from all employees, stakeholders, and external partners. This feedback is collected through regular surveys, suggestion boxes, and during post-incident reviews.

- **Analysis and Integration**: The SSP maintenance team analyzes feedback and integrates actionable suggestions into the plan. This collaborative approach ensures that the SSP benefits from a wide range of perspectives and expertise.

10.3 Documentation and Communication of Changes

- **Change Log**: All changes to the SSP are documented in a change log that includes a description of the change, the reason for the change, and the date it was implemented. This log is accessible to all employees for transparency and accountability.

- **Communication Plan**: Significant updates to the SSP are communicated to all relevant stakeholders through a combination of email announcements, staff meetings, and training sessions. This ensures that all team members are aware of new policies or procedures and understand their roles and responsibilities in maintaining security.

10.4 Training and Awareness Activities

- **Ongoing Education**: Following updates to the SSP, targeted training sessions are held to educate employees on new or revised security policies and procedures. These sessions are designed to ensure that all employees, regardless of their role, understand the importance of the SSP and how it applies to their daily work.

- **Awareness Campaigns**: We also launch awareness campaigns to highlight specific changes in the SSP, focusing on areas of significant impact or where employee action is required. These campaigns use a variety of formats, including posters, intranet articles, and interactive workshops, to engage employees and reinforce key messages.

Section 11: References

This section consolidates all key references and resources that inform and support the System Security Plan (SSP) for the protection of Controlled Unclassified Information (CUI). Our SSP is aligned with best practices and compliance standards to ensure the highest level of security and integrity in managing CUI.

- **NIST Special Publication 800-171**: "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations" outlines the standards for safeguarding CUI on nonfederal information systems. This document is foundational to our security practices and policies.
- **DFARS 252.204-7012**: "Safeguarding Covered Defense Information and Cyber Incident Reporting" mandates defense contractors to protect covered defense information, report cyber

incidents, and adhere to specific cybersecurity requirements. Compliance with DFARS is essential for our operations and reflects our commitment to national defense security standards.
- **GDPR Article 32**: "Security of Processing" under the General Data Protection Regulation outlines the requirements for securing personal data processing activities. This regulation underscores our commitment to protecting personal information within the scope of our global operations.
- **Organization-specific Policies, Standards, and Guidelines**: Our internal documents, including security policies, standards, and guidelines, detail the specific procedures and controls we have implemented. These documents are regularly reviewed and updated to reflect best practices, technological advancements, and changes in the threat landscape.

Appendices

The appendices provide supporting documentation, templates, and additional resources that complement the main body of the System Security Plan (SSP). These documents are critical for implementing, understanding, and adhering to the security measures outlined in the SSP.

Appendix A: Glossary of Terms and Acronyms

- **CUI (Controlled Unclassified Information)**: Information that requires protection under laws, regulations, or government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended.
- **DFARS (Defense Federal Acquisition Regulation Supplement) 252.204-7012**: A clause requiring defense contractors to safeguard covered defense information, report cyber incidents, and submit malicious software to the DoD Cyber Crime Center.
- **NIST (National Institute of Standards and Technology)**: A federal agency within the U.S. Department of Commerce responsible for developing technology, metrics, and standards.
- **SSP (System Security Plan)**: A document that outlines the processes and controls in place to secure a system or information asset.
- **RBAC (Role-Based Access Control)**: A method of restricting system access to authorized users based on their roles within an organization.
- **AES (Advanced Encryption Standard)**: A symmetric encryption algorithm widely used across the globe to protect data.
- **IDPS (Intrusion Detection and Prevention Systems)**: Security applications that monitor network or system activities for malicious activities or policy violations.

Appendix B: Contact Information for Incident Response Team

- **Incident Response Coordinator**: Ryan O'Connor, Email: ryano@911eda.com, Phone: (760) 646-0745
- **IT Security Specialist**: Anthony Pereira, Email: tpereira@911eda.com, Phone: (800) 320-2480 x103
- **Legal Advisor**: John Bray, Email: jbray@braylaw.com, Phone: (760) 941-9134

Appendix C: Regulatory Compliance Matrix

SSP Control	Regulation/Standard	Compliance Note
Incident Reporting	DFARS 252.204-7012	Meets the requirement for rapid reporting of cyber incidents within 72 hours to the DoD.
Access Control	DFARS 252.204-7012	Ensures that access to covered defense information is limited to authorized users in compliance with DFARS mandates.
Network Security	DFARS 252.204-7012	Implements robust monitoring and protection measures for systems containing CUI, aligning with DFARS requirements.
Access Control	NIST SP 800-171	Meets requirements for limiting system access to authorized users.
Data Encryption	GDPR Article 32	Ensures encryption of personal data in transit and at rest.

Appendix D: Training Program Outline

1. **Orientation to CUI Protection**: Introduction to handling and protecting Controlled Unclassified Information, including the significance of DFARS 252.204-7012 compliance.
2. **Password Security Best Practices**: Training on creating strong, secure passwords, using password managers, and understanding the importance of password security.
3. **Recognizing and Reporting Phishing Attempts**: Guidelines on identifying phishing emails and protocols for reporting potential security threats.
4. **Incident Reporting Procedures**: Detailed process for reporting security incidents, emphasizing the timeline and procedures outlined in DFARS 252.204-7012.
5. **DFARS Compliance Training**: A specific session focused on understanding DFARS 252.204-7012 requirements, the importance of swift incident reporting, and safeguarding covered defense information.
6. **Annual Security Refresher**: A mandatory annual training to update employees on new security policies, threats, and technologies.

Appendix E: Change Log for SSP Updates

Version	Date	Description of Changes	Author(s)
1.0	02/17/2019	Initial creation of the System Security Plan (SSP).	SSP Team
1.1	06/15/2019	Updated to include additional encryption protocols.	SSP Team
1.2	12/08/2019	Revised incident response procedures and added new training modules.	SSP Team
1.3	05/23/2020	Enhanced access control measures and updated malware protection solutions.	SSP Team
1.4	11/14/2020	Introduction of continuous monitoring practices.	SSP Team
1.5	04/07/2021	Adjustments to the data handling policy for clarity and compliance.	SSP Team
1.6	08/19/2021	Revision of security awareness training content.	SSP Team
1.7	12/01/2021	Incorporation of feedback mechanism for continuous improvement.	SSP Team
2.0	06/05/2023	Major update to align with the latest NIST SP 800-171 revision.	SSP Team
2.1	11/22/2023	Minor updates to risk assessment procedures and training curriculum.	SSP Team

Appendix F: Feedback Form Template

SSP Feedback Form

We welcome your suggestions for improving our System Security Plan. Please provide your feedback below:

- **Name** (optional): _____
- **Date**: _____
- **Section of SSP** (if applicable): _____
- **Feedback/Suggestion**:

(Please submit this form to the SSP maintenance team via email)