Dale County Commission

Commission Meeting Minutes – September 26, 2023

The Dale County Commission convened in a regular session Tuesday, September 26, 2023. The following members were present: Chairman Steve McKinnon; District Two Commissioner Donald O. Grantham; District Three Commissioner Adam Enfinger; and District Four Commissioner Frankie Wilson. Absent: District One Commissioner Chris Carroll.

Chairman McKinnon called the meeting to order at 10:00am. Commissioner Wilson opened with prayer. Commissioner Grantham followed with the Pledge of Allegiance.

APPROVED – MINUTES & MEMORANDUM OF WARRANTS

Commissioner Enfinger made a motion to approve the memorandum of warrants and minutes:

Memorandum of Warrants:

- Accounts Payable Check Numbers 97177 – 97285.
- Payroll Check Numbers: 154934 – 154938.
- Direct Deposit Check Numbers: 426249 - 426393.

Minutes: Commission Meeting of September 12, 2023.

Commissioner Grantham seconded the motion, all voted aye. Motion carried.

APPROVED – AGENDA

Commissioner Enfinger made a motion to approve the agenda with the deletion of #7- ARPA - Sheriff Office Remodel- Bid Award.

Commissioner Wilson seconded the motion, all voted aye. Motion carried.

APPROVED – PERSONNEL

Commissioner Enfinger made a motion to approve the following:

1. Ashley Lopez – Sheriff – Deputy – transfer from Jail.

Commissioner Wilson seconded the motion, all voted aye. Motion carried.

APPROVED – TRAVEL

Commissioner Wilson made a motion to approve the following:

1. Matt Murphy – Road & Bridge – 09/19-20/23 – Vegetation Mgmt. Training.
2. Steve McKinnon – Commission – 10/25-26/23 – ACCA Legislative Pre-Session.
3. Nathan Ivey – Reappraisal – 11/12-16/23 – AL Real Property Class.
4. David Grubbs – Coroner – 09/25-28/23 – Child Death Investigation.
5. Steve McKinnon, Cheryl Ganey, Matt Murphy – 11/28-30/23 – ACCA Legislative Conference.

Commissioner Grantham seconded the motion, all voted aye. Motion carried.

APPROVED – AMENDMENT TO POLICIES & PROCEDURES

Commissioner Grantham made a motion to approve an amendment to the Dale County Personnel Policy & Procedures Handbook. New Data and Cybersecurity Policy to replace the current information under section XIV-Computer/Email Policy with revised title of Data and Cybersecurity policy. See Exhibit 1.

Commissioner Enfinger seconded the motion, all voted aye. Motion carried.

APPROVED – AMENDMENT TO CLASSIFICATION & PAY PLAN

Commissioner Wilson made a motion to approve an amendment to the Dale County Commission's Classification and Pay Plan. Updated job description for District Administrative Coordinator – Pay Grade X (10). See Exhibit 2.

Commissioner Grantham seconded the motion, all voted aye. Motion carried.

APPROVED – 2022 – 2023 BUDGET AMENDMENTS

Commissioner Enfinger made a motion to approve to the 2022-2023 Dale County Commission budget amendments. Exhibit 3.

Commissioner Grantham seconded the motion, all voted aye. Motion carried.

APPROVED – 2023 – 2024 BUDGET

Commissioner Enfinger made a motion to approve the 2023-2024 Dale County Commission Budget. Exhibit 4.

Commissioner Wilson seconded the motion, all voted aye. Motion carried.

APPROVED – HOT MIX ASPHALT BID AWARD

Commissioner Enfinger made a motion to approve the hot mix asphalt bid. See Exhibit 5.

Commissioner Wilson seconded the motion, all voted aye. Motion carried.

APPROVED – EMA – EMPG GRANT AGREEMENT

Commissioner Enfinger made a motion to approve an EMPG Grant. See Exhibit 6.

Commissioner Wilson seconded the motion, all voted aye. Motion carried.

ANNOUNCEMENT – NEXT REGULAR MEETING

Chairman McKinnon announced that the next regular meeting of the Dale County Commission will be Tuesday, October 10, 2023, at 10:00am.

ADJOURNMENT: CONFIRMATORY STATEMENT

Commissioner Enfinger made a motion to adjourn the meeting. Commissioner Grantham seconded the motion. All voted aye. Motion carried.

It is hereby ordered the foregoing documents, resolutions, etc., be duly confirmed and entered into the minutes of the Dale County Commission as its official actions.

Steve McKinnon, Chairman

Dale County Commission

Data and Cybersecurity Policy

Document Revision History

Date	Version	Modification	Author
09/12/2023	1.0	Initial release (DRAFT)	Foxhill Information Systems, LLC

Table of Contents

1. Introduction

In today's world more and more of our business is conducted online, it is vast and growing. The more we rely on technology to collect, store, and manage information, the more vulnerable we become to severe security breaches. A cyber-attack does not only directly threaten Dale County's confidential data, but it may also ruin the relationships with the public and cause severe legal jeopardy to them and Dale County's reputation. The Alabama Data Breach Notification Act of 2018-396 requires counties to implement and maintain reasonable security measures to protect sensitive personally identifying information (SPII) against a breach of security.

1.1.Purpose

The purpose of this policy is to establish guidelines and best practices to ensure the security and protection of information systems and data within the Dale County government institution.

1.2. Scope

This policy applies to all the Dale County employees, contractors, volunteers remote or onsite, and anyone who has permanent or temporary access to Dale County systems, networks, and data.

1.3. Roles and Responsibilities

1.3.1. Management

Management is responsible for ensuring the implementation and enforcement of this policy and providing necessary resources for cybersecurity measures.

1.3.2. IT Department

The IT department is responsible for developing procedures, implementing technical controls, monitoring systems, and responding to security incidents.

1.3.3. Employees

All employees are responsible for adhering to this policy, following security procedures, and reporting any suspected security incidents.

2. Policy Elements

2.1. Access Control

2.1.1. Overview

Access control is a data security process that enables organizations to manage who is authorized to access data and resources. Secure access control uses policies verify users are who they claim to be and ensures appropriate control access levels are granted to users.

2.1.2. User Accounts

Each user should have a unique account with appropriate access rights based on their job responsibilities. Users are prohibited from sharing accounts unless expressly documented and approved by management.

2.1.3. Passwords

All employees must use strong, unique passwords for their accounts and regularly update them. It is suggested that the usage of passwords with a minimum of 8 characters contain a combination of letters, numbers and symbols as is the current requirement. This minimum level of complexity is susceptible to change due to the evolving threat landscape.

2.1.4. Multi-Factor Authentication (MFA)

For MFA, when you sign into the account for the first time on a new device or app, you need more than just the username and password. You need a second factor to prove who you are. A factor in authentication is a way of confirming your identity when you try to sign in. For example, a password is one kind of factor, it's a thing you know. The three most common kinds of factors are:

- **Knowledge-based factor** – Password, answer to a security question, or a memorized PIN.
- **Possession factor** – Smartphone or USB key.
- **Inherence factor** – Fingerprint or facial recognition.

MFA must be enabled for any administrative level access to systems containing sensitive data, remote access, and while using email provided by Dale County.

2.1.5. Additional Controls

- **Firewalls** – We have deployed enterprise-grade firewalls at strategic points within our network infrastructure to monitor and control incoming and outgoing network traffic. The firewalls are configured to enforce strict access control policies, allowing only authorized traffic to pass through while blocking or flagging suspicious or unauthorized connections. We regularly update and patch the firewall systems to ensure they are equipped with the latest security features and defense mechanisms.
- **Intrusion Detection and Prevention** - We employ intrusion detection and prevention systems (IDS/IPS) to monitor network traffic for potential threats or suspicious activities. These systems employ advanced algorithms and threat intelligence to identify and respond to security incidents promptly. When an intrusion attempt is detected, the IDS/IPS takes immediate action, such as alerting IT or blocking malicious traffic.

2.1.6. Access Control Change Management

Any changes to access controls, including the granting or revocation of access, must be documented and approved by designated personnel. Access reviews should also be conducted periodically to limit authorized access.

2.2. Data protection

2.2.1. Overview

Data protection is the process of protecting sensitive personally identifying information (SPII) from damage, loss, or corruption.

2.2.2. Data confidentiality

Data backups are stored encrypted "at rest" ensuring access is granted to authorized employees. Any unauthorized attempts to access sensitive personally identifying information (SPII) must be reported immediately to designated personnel.

2.2.3. Data integrity

Periodic testing of data backups is performed to ensure usability of data if a recovery is needed.

2.2.4. Data availability

Daily and weekly data backups are in place to automatically distribute important data to online and offline storage

locations to affect quick recovery in the event of a system failure or malicious event causing data loss.

2.3. Incident Response (IR)

2.3.1. Overview

Incident response is the process of dealing with a data breach or cyberattack, including how an organization attempts to control the consequences of such an incident. As referenced above, the Alabama Data Breach Notification Act of 2018-396 requires a written notice be made to affected individuals (and to the Alabama Office of the Attorney General if over 1,000 Alabama residents are notified) within 45 calendar days of a determination that the breach of security is reasonably likely to cause substantial harm to affected individuals. Notice to all consumer reporting agencies is also required "without unreasonable delay" if over 1,000 Alabama residents are notified. The goal is to effectively manage such an incident to minimize damage to the public, county systems and data, reduce recovery time and cost, and control damage to the county's reputation.

2.3.2. IR Team

In the event of a security breach or other incident, a designated incident response team must be formed and activated. The team must have clear roles and responsibilities and must follow established procedures for notification and communication. The team must work to quickly assess the situation, contain, and mitigate the incident, and restore affected systems and data.

2.3.3. Roles and responsibilities

- **Employees** -- All employees should promptly report any suspected or actual security incidents to the IT department.
- **IT** – Collects and analyzes all evidence, determines root cause, and implements rapid system and service recovery. Documents lessons learned for quality assurance.
- **Management** – Leads the effort of messaging and communications for all audiences, inside and outside the county. Reaches out to

HR/Legal/Law Enforcement for representation and guidance if necessary.

2.3.4. Goals of IR

- **Early Detection**: The primary goal of Incident Response is to detect security incidents as early as possible. Early detection can minimize the impact of a security breach and prevent further compromise.
- **Rapid Response:** Once an incident is detected, the IR team must respond swiftly and efficiently. A rapid response can help contain the incident and prevent it from spreading to other parts of the network.
- **Containment**: The IR team's goal is to contain the incident to limit its impact and prevent further damage. This may involve isolating affected systems, disabling compromised accounts, or blocking malicious network traffic.
- **Investigation and Analysis:** Incident Response involves a thorough investigation to understand the scope and nature of the incident. This includes identifying the attack vectors, the extent of data or system compromise, and the tactics used by the attackers.
- **Mitigation:** After analyzing the incident, the IR team works on implementing mitigation strategies to prevent similar incidents in the future. This could include applying patches, updating security configurations, or improving security awareness training for employees.
- **Recovery:** Incident Response aims to restore affected systems and services to their normal state while ensuring that the restoration is done securely to prevent re-infection.
- **Documentation:** Proper documentation of the incident response process is crucial. This includes capturing all the actions taken during the investigation, response, and recovery phases. Documentation helps organizations learn from incidents and improve their cybersecurity posture.
- **Communication:** Effective communication during an incident is vital. The IR team must communicate with internal stakeholders, such as management, IT staff, and employees, as well as external parties, such as law enforcement agencies, partners, and customers.
- **Continuous Improvement:** Incident Response is an ongoing process that requires constant improvement. After each incident, the IR team should conduct a post-mortem analysis to identify

areas for improvement and adjust their incident response plan accordingly.

- **Compliance and Reporting:** Incident Response often involves complying with legal and regulatory requirements. Proper reporting is necessary for compliance purposes and to keep stakeholders informed about the incident and the actions taken to address it.

2.4. Risk Assessment and Management

2.4.1. Asset Identification

Identify all the assets in the Dale County IT environment that need protection, including hardware, software, data, personnel, and facilities. Categorize them based on their criticality and sensitivity.

2.4.2. Threat Identification

Identify potential cybersecurity threats that could exploit vulnerabilities in the assets. These threats may include malware, social engineering, insider threats, hacking, etc.

2.4.3. Vulnerability Assessment

Conduct a comprehensive vulnerability assessment to identify weaknesses in the IT infrastructure, applications, and processes that could be exploited by threats.

2.4.4. Risk Analysis

Assess the potential impact and likelihood of each threat exploiting specific vulnerabilities to cause harm to the IT assets. Assign a risk rating to each threat based on the combination of impact and likelihood.

2.4.5. Risk Evaluation

Prioritize the identified risks based on their severity and potential impact on the county. This step will help focus on addressing the most critical risks first.

2.4.6. Risk Treatment

Develop risk management strategies to mitigate, transfer, avoid, or accept the identified risks. Some common risk treatment options in the context of cybersecurity include:

- **Risk Avoidance**: Eliminate the risk by discontinuing or not engaging in certain high-risk activities or technologies.
- **Risk Mitigation**: Implement measures to reduce the likelihood or impact of the risk. This could involve implementing security controls, updating software, conducting employee training, etc.
- **Risk Transfer**: Shift the risk to a third party, such as through cybersecurity insurance or outsourcing certain functions to specialized providers.
- **Risk Acceptance**: Choose to accept the risk if the cost of mitigating it outweighs the potential impact or if it's deemed acceptable based on the county's risk appetite.

2.4.7. Implementation of Controls

Implement the selected risk treatment strategies and security controls. This may involve investing in cybersecurity tools, updating policies and procedures, and conducting training sessions for employees.

2.4.8. Monitoring and Review

Continuously monitor the IT environment, analyze cybersecurity trends, and review the effectiveness of implemented controls. Regularly update risk assessments as new threats and vulnerabilities emerge.

2.4.9. Continuous Improvement

Cybersecurity is an ongoing process, and threats evolve over time. Continuously learn from past incidents and update the risk assessment and management strategies accordingly.

2.5. Patch Management

2.5.1. What is Patch Management?

Patch management procedures are a crucial aspect of maintaining the security and stability of computer systems and software. The process involves identifying, evaluating, testing, and deploying patches and updates to address vulnerabilities, fix bugs, and improve performance.

2.5.2. Patch Types

A patch within the Dale County environment is classified as either an upgrade or an accumulation of fixes to either a known problem/vulnerability or potential problem/vulnerability within an operating or software system. Furthermore, IT will leverage the Dale County patch management infrastructure to deliver tools to help secure Dale County systems and distribute supported third-party software in the form of patches as described below.

A patch is divided into four (4) different categories:

Category 1 – *Security Patches*
Category 2 – *Non-Security Patches*
Category 3 – *Security Tools*
Category 4 - *Software Distribution*

2.5.3. Roles and Responsibilities

- **Management**:
  - Notify IT of criticality of systems and/or if patching will hinder Dale County operations.
  - Ensure employees leave machines on during patching operational windows.
- **IT**:
  - Send notices out to schedule patching operational windows.
  - Stay informed about the latest patches and updates for your operating system, applications, and software. Regularly check official vendor websites, security advisories, and mailing lists.
  - Assess the severity and relevance of each patch to your organization's environment. Focus on critical security updates first.
  - Monitor systems after patch deployment to ensure the patches were successful and did not cause any unexpected problems.
  - Ensure patch management procedures comply with any relevant security policies, regulations, or industry standards (e.g., GDPR, HIPAA, PCI DSS).

- Schedule regular maintenance windows for patching to minimize disruptions and maximize efficiency.

- **Employees**:
  - Comply with IT policy by leaving machines on as directed by Management and IT.
  - Notify Management and/or IT if unexpected system behavior after patching.

3. Social Media Policy and Procedure

3.1 INTRODUCTION

Social media can be an effective communication tool for the county commission and its instrumentalities, departments, and agencies (collectively "County"). Improper usage of social media, however, may impact the County and affect the public trust in and credibility of the County. The County recognizes and respects the rights of its employees to participate in social media platforms. Employees, however, must ensure that their online content is consistent with the County's standards of conduct.

3.2 PURPOSE

The purpose of this policy is to define the parameters for both official and personal use of social media.

3.3 SCOPE

This policy applies to all county commission offices and county-funded instrumentalities, departments, and agencies, including but not limited to, the Revenue Commissioner's office, the probate office, and any other county-funded entity or program, and applies to permanent and part-time employees, remote workers, third-party agents, contractors, consultants, volunteers, suppliers, interns, and any individuals ("Users") who have permanent or temporary access to the County's social media platforms, sites, or pages. This policy applies to all social media communications whether or not an employee or User is posting under his or her name, anonymously, or through an alias or other means and to such communication and usage on personally-owned devices whether connected by wire or wireless service to

the county network. This policy also applies to social media communication and usage on devices purchased using any officials' discretionary funds.

3.4 DEFINITIONS

3.4.1 SOCIAL MEDIA: All means of communicating or posting information or content of any sort on the Internet, including to your own or someone else's web log or blog, journal or diary, personal web site, social networking or affinity web site, web bulletin board or a chat room, forums, comment sections, and private or direct messages, whether or not associated or affiliated with the County, as well as any other form of electronic communication.

3.4.2 OFFICIAL COUNTY EMAIL ACCOUNT: Email account provided by a County instrumentality, department, or agency mail system or approved external mailbox that is used for official county business.

3.4.3 COUNTY APPROVED SOCIAL MEDIA SITE: A social network that has been assessed and approved by the county administrator, the information technology (IT) department, the county attorney and human resources director, and/or the county department head or agency head.

3.4.4 SOCIAL NETWORK: Online platforms, sites, or pages, where profiles are created, information is shared, and parties socialize with each other using a range of electronic communication and technologies.

3.4.5 PAGE: The portion of the social media network or platform where content is displayed, usually by a person with administrator rights.

3.4.6 POST: A submitted or published message or blog in the form of, but not limited to, text, videos, photographs, graphics, links, including hyperlinks, documents, and computer applications.

3.4.7 PROFILE: Information provided about a person or the County on a social networking platform, site, or page.

3.4.8 COMMENT: A submitted or published response to a post.

3.5 COUNTY SOCIAL MEDIA USE AND MANAGEMENT

County social media usage shall be limited to those with an official County business and purpose to use social media. County-sponsored and social media platforms, sites, or pages for County instrumentalities, departments, and agencies should be reviewed and approved by the county administrator, the information technology (IT) department, the county attorney, the human resources director, and/or the county department head or agency head. Any County-sponsored and approved social media platform, site, or page should be clearly identified with the following phrase: "Official social media site of 'department name," including a link to the County or department website and should include the County, department, or agency logo. A disclaimer should be placed on the platform, site, or page indicating that information included in posts and originating device identification information may be subject to public record disclosure and shall be recorded and archived. The County should designate a person who is responsible for social media communications, including but not limited to, determining what information is posted on the platform(s), site(s), or page(s), and updating, commenting, reviewing, and auditing the content. The County should also identify backup personnel for times the designated person is unavailable. Designated personnel participating in social media discussions related to county business matters during off-County time shall indicate that viewpoints shared are personal and do not necessarily reflect County opinion. Any County-sponsored and approved social media platform(s), site(s), or page(s) should comply with all federal, state, and local laws.

3.6 PERSONAL USE OF SOCIAL MEDIA

3.6.1 Employees have the right to speak and act on social media on their own time as private citizens on matters of public concern. However, the following actions are forbidden, including but not limited to, regardless of whether an employee or User is on his or her own time:

a) Disseminating or discussing any information accessed because of an employee's position that is not generally available to the public, including, but not limited to, confidential information regarding citizens or co-employees, or others; information regarding safety and security plans or procedures; information regarding expected or pending legal matters; or information regarding contract negotiations;
b) Releasing any media including, but not limited to pictures, videos, and audio recordings, obtained during the performance of an employee's, agency-related activities, and agency-responder activities, unless prior approval is obtained;
c) Stating, suggesting, or implying in any manner that an employee or User is acting or speaking on behalf of the County without prior express authorization;
d) Violating the County's policies against harassment or discrimination; and
e) Taking any other action that may reasonably be expected to interfere with the employee's job duties or the County's operations.

3.7 EMAIL AND INTERNET SOCIAL MEDIA USAGE

Employees are generally expected to work during all work times and should refrain from engaging in personal activities during work hours except for breaks. Personal use of electronic mail, social media, etc., that interferes with an employee's performance of his or her job duties is strictly prohibited. Any use of county resources, including, but not limited to, county equipment or bandwidth, for personal use may result in any information regarding the use, including metadata and data, to become public, and employees and Users have a decreased expectation of privacy in personal devices brought onto County property.

4. Data Retention and Disposal

The County follows the County Commissions Functional Analysis & Records Disposition Authority Guidelines as adopted by the Local Government Records Commission. The County will ensure compliance with all necessary legal and regulatory requirements regarding retention, storage, and disposal. When establishing and/or reviewing retention periods, the following will be considered:

- Local Government Records Commission retention, recommendations, and disposition;
- The objectives and requirements of the county;
- The class of data in question;
- The purpose(s) for which the data in question is collected, held, and processed;
- The county's legal basis for collecting, holding, and processing that data; and
- Anticipated or pending litigation.

5. IT Acceptable Usage Policy

Dale County

IT Acceptable Usage Policy

1. Employees will use Dale County-owned IT equipment, including computers, laptops, tablets, phones, and other devices, only for authorized business purposes, not for personal or unauthorized purposes.
2. Internet, email, and other communication tools to access, download, or distribute inappropriate or illegal content. Employees shall not use equipment, including computers, laptops, tablets, phones, and other devices, or any means of communication in violation of any federal or state law or in violation of another county policy.
3. Dale County-owned printers, copiers, or scanners will not be used for personal or unauthorized purposes. These devices will not be used to print or copy large quantities of personal documents or other materials without prior approval.

4. Dale County has the right to monitor and review my use of Dale County-owned equipment, including my internet and email usage. Employees will not attempt to bypass or circumvent any security or monitoring measures in place.
5. Employees will immediately report any issues or concerns with Dale County-owned equipment to designated IT personnel. Employees will also report any suspected security breaches or other unauthorized use of Dale County-owned equipment.
6. Employees understand that any violations of this acceptable use agreement may result in disciplinary action as set out in this policy.

6. Disciplinary Action

Disciplinary action may be taken against employees who violate this policy. Violation of this policy can lead to disciplinary action up to and including termination. The County's disciplinary protocols are based on the severity of the violation. Unintentional violations may only warrant a verbal warning. Frequent violations of the same nature, however, may lead to a written warning. Intentional violations can lead to suspension or termination of employment, depending on the case circumstances. Employees may also be exposed to personal liability.

7. COUNTY AND PERSONAL DEVICE SECURITY

When Users use county or personal devices to access information from the county Data Assets, they introduce security risks to county data. A device means, but is not limited to, a laptop, tablet, personal computer, workstation, smart phone or mobile device.

To ensure the security of all county-issued devices and Data Assets, all Users are required to:

- Keep all county-issued devices password protected;
- Ensure devices are not exposed or left unattended;
- Refrain from sharing private passwords with coworkers, personal acquaintances, or others;
- Ensure devices are current with security patches and updates and regularly updated with the latest anti-virus, anti-malware, or security software;
- Install security updates of browsers and systems monthly or as soon as updates are available;
- Discourage use of others 'devices to access the county's systems, networks, and technology infrastructure;
- Avoid lending county devices to other individuals;
- Use only secure and private networks to log into county systems, networks, and technology infrastructure; and
- Obtain authorization from the County Administrator, IT Manager, or designee before removing devices from county premises.

A personal device means, but is not limited to, a laptop, tablet, personal computer, workstation, smart phone, mobile device, or other device that is authorized to access the county's Data Assets or is used to backup any such device and is owned by a User and acquired voluntarily,

without payment by the county and without any expectation of reimbursement for any costs related to the purchase, activation, operational/connectivity charges, service or repairs, or other costs that may be incurred related to the device or its use. The county recognizes that Users may use personal devices to access the county's Data Assets. In such cases, Users must report this information to the County Administrator, IT Manager, or designee for record-keeping purposes. To ensure the county Data Assets are protected, all Users are required to:

- Ensure all personal devices used to access county-related Data Assets are password protected;
- Lock all devices if unattended;
- Ensure all devices are protected at all times;
- Install and regularly update security patches, anti-virus, anti-malware, and security software; and
- Use only secure and private networks.

8. EMAIL SECURITY

Protecting email systems internally and externally is a high priority as emails can lead to data theft, corruption, virus infections, phishing attacks, and scams. Therefore, the county instructs all Users to:

- Verify the legitimacy of each email, including the email address and sender name;
- Avoid opening suspicious emails, attachments, and links;
- Be suspicious of phishing, clickbait titles and links (e.g., offering prizes, advice);
- Look for inconsistencies or giveaways (e.g., grammatical errors, capital letters, overuse of punctuation marks);
- Delete immediately unsolicited email (spam) from unknown parties; and
- Refrain from using county email for personal use.

Users should contact the County Administrator, IT Manager, or designee regarding any suspicious emails.

9. CLEAR DESK AND SCREEN SECURITY

Users must have an awareness of the importance of keeping both paper and electronic documents and records safe when they are working at their desk, workstation, or screen and have knowledge of how to protect them. This ensures that all sensitive information, whether it be on paper, a storage device, or a hardware device is properly locked away or disposed of when a workstation is not in use. This will reduce the risk of unauthorized access, loss of, and damage to information during and outside of normal business. For a clear desk, Users should operate as follows:

- When leaving a desk for a short period of time, Users must ensure printed matter containing information that is sensitive or confidential is not left in view.

- When leaving a desk for a longer period of time or overnight, Users must ensure printed matter containing sensitive or confidential information is securely locked away.
- Whiteboards and flipcharts must be wiped and removed of all sensitive information.

For a clear screen, Users should operate as follows:

- When leaving the workstation for any period of time, Users must ensure they lock their computer session to prevent unauthorized access to the network and stored information.
- All users must ensure their screens cannot be overlooked by members of the public, or people without the necessary authority when sensitive or confidential data or information is displayed. Where appropriate, privacy filters should be used to protect the information.
- Following up to a maximum of 15 minutes of inactivity, the session will be automatically locked as a failsafe measure.

10. REMOTE ACCESS

Users sometimes access the county's Data Assets from a distance. Secure remote access must be strictly controlled with encryption (e.g., Virtual Private Networks (VPNs)) and strong passwords. It is the responsibility of Users with remote access privileges to the county's network to ensure that their remote access connection is given the same consideration as the User's on-site connection to the county's data network. General access to the internet for personal use through the county network or Data Assets is strictly limited to Users. When accessing the county network from a personal computer, Users are responsible for preventing access to any county Data Assets by other individuals. Performance of illegal activities through the county network or Data Assets by any User is prohibited.

11. PRIVACY

Users shall have no expectation of privacy for any information they store, send, receive, or access on the county's Data Assets. The county may monitor and inspect all Data Assets of any User without prior notice, in the course of an investigation triggered by indications of misconduct, or on random basis.

Exhibit 2

District Administrative Coordinator Job Description

Division	Department	Location
District Soil & Water Conservation	Road and Bridge	Dale County Commission

Reports To
County Engineer

Job Summary

To provide administrative and advanced clerical duties for coordinating the district program. This position also provides administrative and advanced clerical duties assistance to the USDA/NRCS field office staff with the implementation of conservation programs to the public.

Duties and Responsibilities:

1. Assist the District Board in carrying out its administrative responsibilities. Coordinate the District's conservation programs.
2. Serves as receptionist: receives walk-in clients and telephone calls. Answers questions, gives assistance in signing up for various programs and directs clients for assistance to proper office personnel.
3. Serves as bookkeeper for all district accounts. Maintains and prepares all required financial records including processing payroll, taxes filed with the Federal, State, and Social Security. Process W-2 Tax forms and 1099's. Prepares checks and deposits. Provides board members with monthly financial reports and prepares the annual district budget. Prepares quarterly travel vouchers for payment.
4. Assists in preparing Board Meeting Agenda in coordination with the District Conservationist. Provides supervisors with an agenda, monthly financial report, and of previous month's board meeting minutes prior to each monthly board meeting.
5. Attends monthly board meetings. Provides supervisors with all pertinent information for meeting in order to keep supervisors informed of upcoming activities. Records board meeting minutes.
6. Maintains communication between the District and the NRCS field office personnel to assure cooperation and avoid duplication of efforts. Assists NRCS with reports, data entry, program sign-ups, correspondence, filing, recording NRCS Staff Meeting Minutes and arranging appointments.
7. Assist in entering client information into Protracts and Toolkits for NRCS programs.
8. Responsible for registering new AFO/CAFO applicants and re-registering CAFO's on a yearly basis.
9. Other duties as assigned.

Skills and Knowledge

1. Willing to learn aerial photography interpretation, agricultural, wildlife, forestry and miscellaneous minor engineering practices.
2. Skills in public relation with other units of government.
3. Knowledge of written and oral communication techniques to address groups to prepare informational articles, and to prepare summary work reports.
4. Ability to operate a motor vehicle and be insurable.
5. Ability to operate office equipment such as computers, copiers, and fax machines.
6. Ability to work closely with others in a public office environment.
7. Ability to organize and plan own schedule of activities related to work goals.
8. Accounting Skills to manage bank record keeping and IRS records and reports.

Supervisory Responsibilities
None

Physical Demands

Standing
Up to 33%

Walking
Up to 33%

Sitting
More than 66%

Stooping, Kneeling, Crouching,
33 - 66%

Climbing or Balancing
Up to 33%

Use Hands to Finger, Handle,
More than 66%

Reaching with Hands and Arms
More than 66%

Talking or Hearing
More than 66%

Lifting	**Up to 10lbs**	**Up to 25lbs**
Up to 33%	Up to 33%	Up to 33%

Specific physical duties
Must see well enough to read fine print and numbers. Must hear well enough to understand verbal communication. Must have the strength to lift heavy books and the body mobility to move around the office.

Specific Noise Duties
Exposure to general office environment.

Comments
Must be willing to wear appropriate attire and work overtime as needed. Must travel occasionally to attend seminars and training.

Exhibit 2

FYE 23 Budget Amendments

9/26/2023

FUND	DEPARTMENT	ACCOUNT NUMBER	DESCRIPTION	CURRENT BUDGET	ADDITIONAL REVENUE	ADDITIONAL EXPENDITURE	REVISED BUDGET
001- GENERAL	Commission	001-51100-125	workers comp	2,001.31		3,000.00	5,001.31
001- GENERAL	Commission	001-51100-182	professional services	25,000.00		10,000.00	35,000.00
001- GENERAL	Commission	001-51100-234	repairs/maintenance vehicles	0.00		5,000.00	5,000.00
001- GENERAL	Commission	001-51100-251	telephone	35,000.00		15,000.00	50,000.00
001- GENERAL	Bd of Registars	001-51920-180	gis system	9,600.00		4,000.00	13,600.00
001- GENERAL	Courthouse Maint	001-51995-231	r & m to bldgs	15,000.00		40,000.00	55,000.00
001- GENERAL	Maintenance Bldg	001-51997-231	r & m to bldgs	300.00		4,000.00	4,300.00
001- GENERAL	Creel Richardson Main	001-51998-231	r & m to bldgs	10,000.00		6,000.00	16,000.00
001- GENERAL	Government Bldg Maint	001-51999-231	r & m to bldgs	6,000.00		8,000.00	14,000.00
001- GENERAL	Sheriff	001-52100-234	repairs/maintenance vehicles	75,000.00		20,000.00	95,000.00
001- GENERAL	Sheriff -Helicopter	001-52105-274	General Liab ins	16,000.00		7,500.00	23,500.00
001- GENERAL	Sheriff - Impound Lot	001-52115-244	electricity	2,500.00		2,000.00	4,500.00
001- GENERAL	Jail	001-52200-116	overtime	35,000.00		90,000.00	125,000.00
001- GENERAL	Jail	001-52200-121	overtime	80,770.64		11,000.00	91,770.64
001- GENERAL	Coroner	001-52400-182	professional services	15,000.00		10,000.00	25,000.00
001- GENERAL	Coroner	001-52400-234	repairs/maintenance vehicles	3,100.00		4,000.00	7,100.00
001- GENERAL	Dept of Youth Services	001-52610-182	professional services	344,000.00		100,000.00	444,000.00
001- GENERAL	Sr Citizens Power	001-56202-271	insurance on bldgs	2,500.00		1,100.00	3,600.00
001- GENERAL	Family Service Center	001-56904-271	insurance on bldgs	2,300.00		500.00	2,800.00
001- GENERAL	General Fund Balance			0.00	419,484.99		419,484.99
220-REBUILD AL	Rebuild AL Fund balance			44,381.32	355,618.68		400,000.00
221-FEDERAL	Federal Fund Balance			0.00	250,000.00		250,000.00
511 - SOLID WASTE	Fund 511- SOLID WASTE	511-54100-122	health ins	21,254.40		11,000.00	32,254.40
511 - SOLID WASTE	Fund 511- SOLID WASTE	511-54100-186	SW collection charges	1,036,201.88		25,000.00	1,061,201.88
511 - SOLID WASTE	Solid Waste Fund Balance		Fund Balance	15,019.88	36,000.00		51,019.88
512 - LAND FILL	Landfill Fund Balance		Fund Balance	70,000.00	38,983.60		108,983.60

Exhibit 3

DALE COUNTY COMMISSION - 2023-2024 Budget

001 GENERAL FUND

Beginning Fund Balance			591,543.68
Estimated Revenues	6,928,767.48		
Estimated Other Sources	1,675,000.00		
ESTIMATED TOTAL REVENUES AND OTHER SOURCES		8,603,767.48	
Expenditures	(9,095,311.16)		
Estimated Other Uses	(100,000.00)		
ESTIMATED TOTAL EXPENDITURES AND OTHER USES		(9,195,311.16)	
Net RevenuesOther Sources less Expenditures/Other Uses			(591,543.68)
Ending Fund Balance			0.00

050 SHERIFF'S SERVICE OF PROCESS FEE FUND

Beginning Fund Balance			0.00
Estimated Revenues	75,000.00		
Estimated Other Sources	100,000.00		
ESTIMATED TOTAL REVENUES AND OTHER SOURCES		175,000.00	
Expenditures	(175,000.00)		
Estimated Other Uses	0.00		
ESTIMATED TOTAL EXPENDITURES AND OTHER USES		(175,000.00)	
Net RevenuesOther Sources less Expenditures/Other Uses			0.00
Ending Fund Balance			0.00

110 ECONOMIC DEVELOPMENT

Beginning Fund Balance			250,000.00
Estimated Revenues	105,000.00		
Estimated Other Sources	0.00		
ESTIMATED TOTAL REVENUES AND OTHER SOURCES		105,000.00	
Expenditures	(355,000.00)		
Estimated Other Uses	0.00		
ESTIMATED TOTAL EXPENDITURES AND OTHER USES		(355,000.00)	
Net RevenuesOther Sources less Expenditures/Other Uses			(250,000.00)
Ending Fund Balance			0.00

111 GAS TAX FUND

Beginning Fund Balance			1,000,000.00
Estimated Revenues	1,811,920.00		
Estimated Other Sources	0.00		
ESTIMATED TOTAL REVENUES AND OTHER SOURCES		1,811,920.00	
Expenditures	(2,811,920.00)		
Estimated Other Uses	0.00		
ESTIMATED TOTAL EXPENDITURES AND OTHER USES		(2,811,920.00)	
Net RevenuesOther Sources less Expenditures/Other Uses			(1,000,000.00)
Ending Fund Balance			0.00

112 PUBLIC BUILDING ROAD & BRIDGE FUND

Beginning Fund Balance			300,000.00
Estimated Revenues	1,526,000.00		
Estimated Other Sources	0.00		
ESTIMATED TOTAL REVENUES AND OTHER SOURCES		1,526,000.00	
Expenditures	(326,000.00)		
Estimated Other Uses	(1,500,000.00)		
ESTIMATED TOTAL EXPENDITURES AND OTHER USES		(1,826,000.00)	
Net RevenuesOther Sources less Expenditures/Other Uses			(300,000.00)
Ending Fund Balance			0.00

113 PUBLIC HIGHWAY & TRAFFIC FUND

Beginning Fund Balance			0.00
Estimated Revenues	175,000.00		
Estimated Other Sources	0.00		
ESTIMATED TOTAL REVENUES AND OTHER SOURCES		175,000.00	
Expenditures	0.00		
Estimated Other Uses	(175,000.00)		
ESTIMATED TOTAL EXPENDITURES AND OTHER USES		(175,000.00)	
Net RevenuesOther Sources less Expenditures/Other Uses			0.00
Ending Fund Balance			0.00

116 CAPITAL IMPROVEMENT FUND

Beginning Fund Balance			450,000.00	
Estimated Revenues	325,000.00			
Estimated Other Sources	0.00			
ESTIMATED TOTAL REVENUES AND OTHER SOURCES		325,000.00		
Expenditures	(586,125.00)			
Estimated Other Uses	(188,875.00)			
ESTIMATED TOTAL EXPENDITURES AND OTHER USES		(775,000.00)		
Net RevenuesOther Sources less Expenditures/Other Uses			(450,000.00)	
Ending Fund Balance				0.00

117 RRR GAS TAX FUND

Beginning Fund Balance			500,000.00	
Estimated Revenues	1,129,000.00			
Estimated Other Sources	300,000.00			
ESTIMATED TOTAL REVENUES AND OTHER SOURCES		1,429,000.00		
Expenditures	(1,929,000.00)			
Estimated Other Uses	0.00			
ESTIMATED TOTAL EXPENDITURES AND OTHER USES		(1,929,000.00)		
Net RevenuesOther Sources less Expenditures/Other Uses			(500,000.00)	
Ending Fund Balance				0.00

119 FIVE CENT GAS TAX FUND

Beginning Fund Balance			0.00	
Estimated Revenues	300,000.00			
Estimated Other Sources	0.00			
ESTIMATED TOTAL REVENUES AND OTHER SOURCES		300,000.00		
Expenditures	0.00			
Estimated Other Uses	(300,000.00)			
ESTIMATED TOTAL EXPENDITURES AND OTHER USES		(300,000.00)		
Net RevenuesOther Sources less Expenditures/Other Uses			0.00	
Ending Fund Balance				0.00

151 AD VALOREM (JAIL TAX) FUND

Beginning Fund Balance			500,000.00
Estimated Revenues	215,000.00		
Estimated Other Sources	0.00		
ESTIMATED TOTAL REVENUES AND OTHER SOURCES		215,000.00	
Expenditures	(715,000.00)		
Estimated Other Uses	0.00		
ESTIMATED TOTAL EXPENDITURES AND OTHER USES		(715,000.00)	
Net RevenuesOther Sources less Expenditures/Other Uses			(500,000.00)
Ending Fund Balance			0.00

220 REBUILD ALABAMA

Beginning Fund Balance			0.00
Estimated Revenues	980,000.00		
Estimated Other Sources	0.00		
ESTIMATED TOTAL REVENUES AND OTHER SOURCES		980,000.00	
Expenditures	(980,000.00)		
Estimated Other Uses	0.00		
ESTIMATED TOTAL EXPENDITURES AND OTHER USES		(980,000.00)	
Net RevenuesOther Sources less Expenditures/Other Uses			(0.00)
Ending Fund Balance			0.00

221 FEDERAL

Beginning Fund Balance			0.00
Estimated Revenues	400,000.00		
Estimated Other Sources	0.00		
ESTIMATED TOTAL REVENUES AND OTHER SOURCES		400,000.00	
Expenditures	(400,000.00)		
Estimated Other Uses	0.00		
ESTIMATED TOTAL EXPENDITURES AND OTHER USES		(400,000.00)	
Net RevenuesOther Sources less Expenditures/Other Uses			0.00
Ending Fund Balance			0.00

301 2014 GENERAL OBLIGATION FUND

Beginning Fund Balance			0.00	
Estimated Revenues	0.00			
Estimated Other Sources	188,875.00			
ESTIMATED TOTAL REVENUES AND OTHER SOURCES		188,875.00		
Expenditures	(188,875.00)			
Estimated Other Uses	0.00			
ESTIMATED TOTAL EXPENDITURES AND OTHER USES		(188,875.00)		
Net RevenuesOther Sources less Expenditures/Other Uses			0.00	
Ending Fund Balance				0.00

511 SOLID WASTE FUND

Beginning Fund Balance			0.00	
Estimated Revenues	1,354,500.00			
Estimated Other Sources	0.00			
ESTIMATED TOTAL REVENUES AND OTHER SOURCES		1,354,500.00		
Expenditures	(1,354,500.00)			
Estimated Other Uses	0.00			
ESTIMATED TOTAL EXPENDITURES AND OTHER USES		(1,354,500.00)		
Net RevenuesOther Sources less Expenditures/Other Uses			0.00	
Ending Fund Balance				0.00

512 LANDFILL FUND

Beginning Fund Balance			61,200.00	
Estimated Revenues	1,500.00			
Estimated Other Sources	0.00			
ESTIMATED TOTAL REVENUES AND OTHER SOURCES		1,500.00		
Expenditures	(62,700.00)			
Estimated Other Uses	0.00			
ESTIMATED TOTAL EXPENDITURES AND OTHER USES		(62,700.00)		
Net RevenuesOther Sources less Expenditures/Other Uses			(61,200.00)	
Ending Fund Balance				0.00

298 AMERICAN RESCUE PLAN

Beginning Fund Balance			6,000,000.00
Estimated Revenues	0.00		
Estimated Other Sources	0.00		
ESTIMATED TOTAL REVENUES AND OTHER SOURCES		0.00	
Expenditures	(6,000,000.00)		
Estimated Other Uses	0.00		
ESTIMATED TOTAL EXPENDITURES AND OTHER USES		(6,000,000.00)	
Net RevenuesOther Sources less Expenditures/Other Uses			(6,000,000.00)
Ending Fund Balance			0.00

031 OPIOID

Beginning Fund Balance			25,000.00
Estimated Revenues	25,000.00		
Estimated Other Sources	0.00		
ESTIMATED TOTAL REVENUES AND OTHER SOURCES		25,000.00	
Expenditures	(50,000.00)		
Estimated Other Uses	0.00		
ESTIMATED TOTAL EXPENDITURES AND OTHER USES		(50,000.00)	
Net RevenuesOther Sources less Expenditures/Other Uses			(25,000.00)
Ending Fund Balance			0.00

Exhibit 5

202 S. Hwy 123, Suite A
Ozark, Alabama 36360
334.774.7875

Matthew W. Murphy, P.E.
County Engineer

DALE COUNTY ROAD AND BRIDGE

MEMORANDUM

Date: September 26, 2023

To: Dale County Commission

From: Matt Murphy
County Engineer

Re: Hot Mix Asphalt

After a careful review, it is the recommendation of the Dale County Engineering Department to award the 2023-2024 Hot Mix Asphalt bid to:

Wiregrass Construction Company, Inc.
PO Box 48
Ariton, AL 36311

HOT MIX ASPHALT 2023-2024

	Mid-South Paving, Inc.	Lewis, Inc.	Wiregrass Construction
DESCRIPTION	**Price Per Ton**	**Price Per Ton**	**Price Per Ton**
Hot Asphalt Plant Mix 424A-340	$95.00	$84.00	$82.00
Hot Asphalt Plant Mix 424A-341	$90.00	$84.00	$82.00
Hot Asphalt Plant Mix 424A-338	$85.00	$84.00	$82.00
Hot Asphalt Plant Mix 424A-346	$85.00	$84.00	$82.00
Balance Mix Design 1/2" Maximum Aggregate Size Mix	$87.00	$86.00	$84.00
Balance Mix Design 3/4" Maximum Aggregate Size Mix	$87.00	$86.00	$84.00
Balance Mix Design, Leveling 3/8" Maximum Aggregate Size Mix	$87.00	$86.00	$84.00
Balance Mix Design, Leveling, 1/2" Maximum Aggregate Size Mix	$87.00	$86.00	$84.00

Exhibit 5

ALABAMA EMERGENCY MANAGEMENT AGENCY (AEMA)
FY2023 EMERGENCY MANAGEMENT PERFORMANCE GRANT (EMPG)
COOPERATIVE AGREEMENT (CA)

1. Subrecipient:	**Dale County EMA**
2. Effective Dates:	**10/01/2022-09/30/2023**
3. Issuing Agency:	**Alabama Emergency Management Agency, 5898 County Road 41, P.O. Drawer 2160, Clanton, AL 35046-2160**
4. FAIN:	**EMA-2023-EP-00005**
5. CA Number(s):	**23EMF**
6. Local Allocation Amount:	**$28,000.00**
7. CFDA #:	**97.042**
8. Federal Award Date:	**09/12/2023**
9. Federal Award Type:	**FY2023 EMPG**

Subrecipient agrees to: (1) provide information requested by AEMA regarding the subrecipient's emergency management operation in a timely manner; (2) submit requests for reimbursement of expenditures incurred relative to this agreement using forms provided or approved by AEMA and utilize the AEMA Grants Management online portal; (3) present claims with clear and adequate supporting documentation as instructed by AEMA; (4) submit claims on a monthly basis within thirty (30) calendar days after the end of the month for which they are filed; (5) submit **all** claims relating to this grant by October 31, 2023; (6) provide information requested by AEMA concerning claimed expenditures within three (3) working days; (7) utilize funds for essential operating expenses of local EMA offices, such as salaries, benefits, supplies, maintenance of facilities, and other necessary and eligible operating costs; (8) make available to AEMA all EMPG related files and documentation for compliance monitoring and review; (9) comply with all reporting, data collection, and evaluation requirements, as prescribed by law or detailed in program guidance; and (10) contribute 50% of all costs submitted for reimbursement as a cash match consisting of payments made by the subrecipient.

The AEMA Director or his/her designated agent may elect to withhold, or, with a ten (10) day notice, withdraw all or part of this funding from the subrecipient for: (1) non-compliance with any portion of the terms stated, referenced, or incorporated into this agreement; (2) failure to perform appropriately in an emergency situation; or, (3) allowing the position of local EMA Director to remain vacant for more than thirty (30) days without appointment of either a new Director or an Acting Director.

Willie T. Worsham WILLIE T. WORSHAM 21 Sep 2023

Local EMA Director (print name, sign, and initial each attached page) Date

Certification by County Authorizing Official:

I certify that I understand and agree to comply with the general and fiscal provisions of this agreement including the terms and conditions; to comply with provisions of the regulations governing these funds and all other applicable federal and state laws; that all information presented is correct; that there has been appropriate coordination with affected agencies; that I am duly authorized to perform the tasks of the Authorizing Official as they relate to the requirements of this agreement; that costs incurred prior to award of funds may result in the expenditures being absorbed by the subrecipient; and, that the receipt of these grant funds through the subrecipient will not supplant other state or local funds budgeted for emergency management purposes.

STEVE McKINNON Steve McKinnon 9/21/22

Chief Elected Official (print name and sign) Date

Jeff Smitherman

Jeff Smitherman, Director, AEMA Date

FY 2023 DHS Standard Terms and Conditions

The Fiscal Year (FY) 2023 DHS Standard Terms and Conditions apply to all new federal financial assistance awards funded in FY 2023. These terms and conditions flow down to subrecipients unless an award term or condition specifically indicates otherwise. The United States has the right to seek judicial enforcement of these obligations.

All legislation and digital resources are referenced with no digital links. The FY 2023 DHS Standard Terms and Conditions will be housed on dhs.gov at www.dhs.gov/publication/fy15-dhs-standard-terms-and-conditions.

A. Assurances, Administrative Requirements, Cost Principles, Representations and Certifications

I. DHS financial assistance recipients must complete either the Office of Management and Budget (OMB) Standard Form 424B Assurances – Non-Construction Programs, or OMB Standard Form 424D Assurances – Construction Programs, as applicable. Certain assurances in these documents may not be applicable to your program, and the DHS financial assistance office (DHS FAO) may require applicants to certify additional assurances. Applicants are required to fill out the assurances as instructed by the awarding agency.

II. DHS financial assistance recipients are required to follow the applicable provisions of the Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards located at Title 2, Code of Federal Regulations (C.F.R.) Part 200 and adopted by DHS at 2 C.F.R. Part 3002.

III. By accepting this agreement, recipients, and their executives, as defined in 2 C.F.R. § 170.315, certify that their policies are in accordance with OMB's guidance located at 2 C.F.R. Part 200, all applicable federal laws, and relevant Executive guidance.

B. General Acknowledgements and Assurances

All recipients, subrecipients, successors, transferees, and assignees must acknowledge and agree to comply with applicable provisions governing DHS access to records, accounts, documents, information, facilities, and staff.

I. Recipients must cooperate with any DHS compliance reviews or compliance investigations conducted by DHS.

II. Recipients must give DHS access to examine and copy records, accounts, and other documents and sources of information related to the federal financial assistance award and permit access to facilities or personnel.

III. Recipients must submit timely, complete, and accurate reports to the appropriate DHS officials and maintain appropriate backup documentation to support the reports.

IV. Recipients must comply with all other special reporting, data collection, and evaluation requirements, as prescribed by law, or detailed in program guidance.

V. Recipients (as defined in 2 C.F.R. Part 200 and including recipients acting as pass-through entities) of federal financial assistance from DHS or one of its awarding component agencies must complete the DHS Civil Rights Evaluation Tool within thirty (30) days of receipt of the Notice of Award for the first award under which this term applies. Recipients of multiple awards of DHS financial assistance should only submit one completed tool for their organization, not per award. After the initial submission, recipients are required to complete the tool once every two (2) years if they have an active award, not every time an award is made. Recipients should submit the completed tool, including supporting materials, to CivilRightsEvaluation@hq.dhs.gov. This tool clarifies the civil rights obligations and related reporting requirements contained in the DHS Standard Terms and

FY 2023 DHS Standard Terms and Conditions

Conditions. Subrecipients are not required to complete and submit this tool to DHS. The evaluation tool can be found at https://www.dhs.gov/publication/dhs-civil-rights-evaluation-tool. DHS Civil Rights Evaluation Tool | Homeland Security

The DHS Office for Civil Rights and Civil Liberties will consider, in its discretion, granting an extension if the recipient identifies steps and a timeline for completing the tool. Recipients should request extensions by emailing the request to CivilRightsEvaluation@hq.dhs.gov prior to expiration of the 30-day deadline.

C. Standard Terms & Conditions

I. Acknowledgement of Federal Funding from DHS

Recipients must acknowledge their use of federal funding when issuing statements, press releases, requests for proposal, bid invitations, and other documents describing projects or programs funded in whole or in part with federal funds.

II. Activities Conducted Abroad

Recipients must ensure that project activities performed outside the United States are coordinated as necessary with appropriate government authorities and that appropriate licenses, permits, or approvals are obtained.

III. Age Discrimination Act of 1975

Recipients must comply with the requirements of the Age Discrimination Act of 1975, Public Law 94-135 (1975) (codified as amended at Title 42, U.S. Code, § 6101 et seq.), which prohibits discrimination on the basis of age in any program or activity receiving federal financial assistance.

IV. Americans with Disabilities Act of 1990

Recipients must comply with the requirements of Titles I, II, and III of the Americans with Disabilities Act, Pub. L. 101-336 (1990) (codified as amended at 42 U.S.C. §§ 12101– 12213), which prohibits recipients from discriminating on the basis of disability in the operation of public entities, public and private transportation systems, places of public accommodation, and certain testing entities.

V. Best Practices for Collection and Use of Personally Identifiable Information

Recipients who collect personally identifiable information (PII) are required to have a publicly available privacy policy that describes standards on the usage and maintenance of the PII they collect. DHS defines PII as any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual. Recipients may also find the DHS Privacy Impact Assessments: Privacy Guidance and Privacy Template as useful resources respectively.

VI. Civil Rights Act of 1964 – Title VI

Recipients must comply with the requirements of Title VI of the Civil Rights Act of 1964 (codified as amended at 42 U.S.C. § 2000d et seq.), which provides that no person in the United States will, on the grounds of race, color, or national origin, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any program or activity receiving federal financial assistance. DHS implementing regulations for the Act are found at 6 C.F.R. Part 21 and 44 C.F.R. Part 7.

VII. Civil Rights Act of 1968

Recipients must comply with Title VIII of the Civil Rights Act of 1968, Pub. L. 90-284, as amended through Pub. L. 113-4, which prohibits recipients from discriminating in the sale, rental, financing, and advertising of dwellings, or in the provision of services in connection

Initial

FY 2023 DHS Standard Terms and Conditions

therewith, on the basis of race, color, national origin, religion, disability, familial status, and sex (see 42 U.S.C. § 3601 et seq.), as implemented by the U.S. Department of Housing and Urban Development at 24 C.F.R. Part 100. The prohibition on disability discrimination includes the requirement that new multifamily housing with four or more dwelling units—i.e., the public and common use areas and individual apartment units (all units in buildings with elevators and ground-floor units in buildings without elevators)—be designed and constructed with certain accessible features. (See 24 C.F.R. Part 100, Subpart D.)

VIII. Copyright

Recipients must affix the applicable copyright notices of 17 U.S.C. §§ 401 or 402 and an acknowledgement of U.S. Government sponsorship (including the award number) to any work first produced under federal financial assistance awards.

IX. Debarment and Suspension

Recipients are subject to the non-procurement debarment and suspension regulations implementing Executive Orders (E.O.) 12549 and 12689, which are at 2 C.F.R. Part 180 as adopted by DHS at 2 C.F.R. Part 3002. These regulations restrict federal financial assistance awards, subawards, and contracts with certain parties that are debarred, suspended, or otherwise excluded from or ineligible for participation in federal assistance programs or activities.

X. Drug-Free Workplace Regulations

Recipients must comply with drug-free workplace requirements in Subpart B (or Subpart C, if the recipient is an individual) of 2 C.F.R. Part 3001, which adopts the Government-wide implementation (2 C.F.R. Part 182) of Sec. 5152-5158 of the Drug-Free Workplace Act of 1988 (41 U.S.C. §§ 8101-8106).

XI. Duplication of Benefits

Any cost allocable to a particular federal financial assistance award provided for in 2 C.F.R. Part 200, Subpart E may not be charged to other federal financial assistance awards to overcome fund deficiencies; to avoid restrictions imposed by federal statutes, regulations, or federal financial assistance award terms and conditions; or for other reasons. However, these prohibitions would not preclude recipients from shifting costs that are allowable under two or more awards in accordance with existing federal statutes, regulations, or the federal financial assistance award terms and conditions may not be charged to other federal financial assistance awards to overcome fund deficiencies; to avoid restrictions imposed by federal statutes, regulations, or federal financial assistance award terms and conditions; or for other reasons.

XII. Education Amendments of 1972 (Equal Opportunity in Education Act) – Title IX

Recipients must comply with the requirements of Title IX of the Education Amendments of 1972, Pub. L. 92-318 (1972) (codified as amended at 20 U.S.C. § 1681 et seq.), which provide that no person in the United States will, on the basis of sex, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any educational program or activity receiving federal financial assistance. DHS implementing regulations are codified at 6 C.F.R. Part 17 and 44 C.F.R. Part 19.

XIII. E.O. 14074 – Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety

Recipient State, Tribal, local, or territorial law enforcement agencies must comply with the requirements of section 12(c) of E.O. 14074. Recipient State, Tribal, local, or territorial law enforcement agencies are also encouraged to adopt and enforce policies consistent with E.O. 14074 to support safe and effective policing.

FY 2023 DHS Standard Terms and Conditions

XIV. Energy Policy and Conservation Act

Recipients must comply with the requirements of the Energy Policy and Conservation Act, Pub. L. 94- 163 (1975) (codified as amended at 42 U.S.C. § 6201 et seq.), which contain policies relating to energy efficiency that are defined in the state energy conservation plan issued in compliance with this Act.

XV. False Claims Act and Program Fraud Civil Remedies

Recipients must comply with the requirements of the False Claims Act, 31 U.S.C. §§3729-3733, which prohibit the submission of false or fraudulent claims for payment to the Federal Government. (See 31 U.S.C. §§ 3801-3812, which details the administrative remedies for false claims and statements made.)

XVI. Federal Debt Status

All recipients are required to be non-delinquent in their repayment of any federal debt. Examples of relevant debt include delinquent payroll and other taxes, audit disallowances, and benefit overpayments. (See OMB Circular A-129.)

XVII. Federal Leadership on Reducing Text Messaging while Driving

Recipients are encouraged to adopt and enforce policies that ban text messaging while driving as described in E.O. 13513, including conducting initiatives described in Section 3(a) of the Order when on official government business or when performing any work for or on behalf of the Federal Government.

XVIII. Fly America Act of 1974

Recipients must comply with Preference for U.S. Flag Air Carriers (air carriers holding certificates under 49 U.S.C.) for international air transportation of people and property to the extent that such service is available, in accordance with the International Air Transportation Fair Competitive Practices Act of 1974, 49 U.S.C. § 40118, and the interpretative guidelines issued by the Comptroller General of the United States in the March 31, 1981, amendment to Comptroller General Decision B-138942.

XIX. Hotel and Motel Fire Safety Act of 1990

Recipients must ensure that all conference, meeting, convention, or training space funded in whole or in part with federal funds complies with the fire prevention and control guidelines of Section 6 of the Hotel and Motel Fire Safety Act of 1990, 15 U.S.C. § 2225a

XX. John S. McCain National Defense Authorization Act of Fiscal Year 2019

Recipients, subrecipients, and their contractors and subcontractors are subject to the prohibitions described in section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232 (2018) and 2 C.F.R. §§ 200.216, 200.327, 200.471, and Appendix II to 2 C.F.R. Part 200. Beginning August 13, 2020, the statute – as it applies to DHS recipients, subrecipients, and their contractors and subcontractors – prohibits obligating or expending federal award funds on certain telecommunications and video surveillance products and contracting with certain entities for national security reasons.

XXI. Limited English Proficiency (Civil Rights Act of 1964, Title VI)

Recipients must comply with Title VI of the Civil Rights Act of 1964, (42 U.S.C. § 2000d et seq.) prohibition against discrimination on the basis of national origin, which requires that recipients of federal financial assistance take reasonable steps to provide meaningful access to persons with limited English proficiency (LEP) to their programs and services. For additional assistance and information regarding language access obligations, please refer to the DHS Recipient Guidance: https://www.dhs.gov/guidance- published-help-department- supported-organizations-provide-meaningful-access-people-limited and additional resources on http://www.lep.gov.

Initial

FY 2023 DHS Standard Terms and Conditions

XXII. Lobbying Prohibitions

Recipients must comply with 31 U.S.C. § 1352, which provides that none of the funds provided under a federal financial assistance award may be expended by the recipient to pay any person to influence, or attempt to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with any federal action related to a federal award or contract, including any extension, continuation, renewal, amendment, or modification.

XXIII. National Environmental Policy Act

Recipients must comply with the requirements of the National Environmental Policy Act of 1969, (NEPA) Pub. L. 91-190 (1970) (codified as amended at 42 U.S.C. § 4321 et seq. and the Council on Environmental Quality (CEQ) Regulations for Implementing the Procedural Provisions of NEPA, which require recipients to use all practicable means within their authority, and consistent with other essential considerations of national policy, to create and maintain conditions under which people and nature can exist in productive harmony and fulfill the social, economic, and other needs of present and future generations of Americans.

XXIV. Nondiscrimination in Matters Pertaining to Faith-Based Organizations

It is DHS policy to ensure the equal treatment of faith-based organizations in social service programs administered or supported by DHS or its component agencies, enabling those organizations to participate in providing important social services to beneficiaries. Recipients must comply with the equal treatment policies and requirements contained in 6 C.F.R. Part 19 and other applicable statues, regulations, and guidance governing the participations of faith- based organizations in individual DHS programs.

XXV. Non-Supplanting Requirement

Recipients receiving federal financial assistance awards made under programs that prohibit supplanting by law must ensure that federal funds do not replace (supplant) funds that have been budgeted for the same purpose through non-federal sources.

XXVI. Notice of Funding Opportunity Requirements

All the instructions, guidance, limitations, and other conditions set forth in the Notice of Funding Opportunity (NOFO) for this program are incorporated here by reference in the award terms and conditions. All recipients must comply with any such requirements set forth in the program NOFO.

XXVII. Patents and Intellectual Property Rights

Recipients are subject to the Bayh-Dole Act, 35 U.S.C. § 200 et seq, unless otherwise provided by law. Recipients are subject to the specific requirements governing the development, reporting, and disposition of rights to inventions and patents resulting from federal financial assistance awards located at 37 C.F.R. Part 401 and the standard patent rights clause located at 37 C.F.R. § 401.14.

XXVIII. Procurement of Recovered Materials

States, political subdivisions of states, and their contractors must comply with Section 6002 of the Solid Waste Disposal Act, Pub. L. 89-272 (1965), (codified as amended by the Resource Conservation and Recovery Act, 42 U.S.C. § 6962.) The requirements of Section 6002 include procuring only items designated in guidelines of the Environmental Protection Agency (EPA) at 40 C.F.R. Part 247 that contain the highest percentage of recovered materials practicable, consistent with maintaining a satisfactory level of competition.

XXIX. Rehabilitation Act of 1973

Recipients must comply with the requirements of Section 504 of the Rehabilitation Act of 1973, Pub. L. 93-112 (1973), (codified as amended at 29 U.S.C. § 794,) which provides

Initial

FY 2023 DHS Standard Terms and Conditions

that no otherwise qualified handicapped individuals in the United States will, solely by reason of the handicap, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any program or activity receiving federal financial assistance.

XXX. Reporting of Matters Related to Recipient Integrity and Performance

General Reporting Requirements:

If the total value of any currently active grants, cooperative agreements, and procurement contracts from all federal awarding agencies exceeds $10,000,000 for any period of time during the period of performance of this federal award, then the recipients must comply with the requirements set forth in the government-wide Award Term and Condition for Recipient Integrity and Performance Matters located at 2 C.F.R. Part 200, Appendix XII, the full text of which is incorporated here by reference in the award terms and conditions.

XXXI. Reporting Subawards and Executive Compensation

Reporting of first tier subawards.

Recipients are required to comply with the requirements set forth in the government-wide award term on Reporting Subawards and Executive Compensation located at 2 C.F.R. Part 170, Appendix A, the full text of which is incorporated here by reference in the award terms and conditions.

XXXII. Required Use of American Iron, Steel, Manufactured Products, and Construction Materials

Recipients must comply with the "Build America, Buy America" provisions of the Infrastructure Investment and Jobs Act and E.O. 14005. Recipients of an award of Federal financial assistance from a program for infrastructure are hereby notified that none of the funds provided under this award may be used for a project for infrastructure unless:

(1) all iron and steel used in the project are produced in the United States—this means all manufacturing processes, from the initial melting stage through the application of coatings, occurred in the United States;

(2) all manufactured products used in the project are produced in the United States—this means the manufactured product was manufactured in the United States; and the cost of the components of the manufactured product that are mined, produced, or manufactured in the United States is greater than 55 percent of the total cost of all components of the manufactured product, unless another standard for determining the minimum amount of domestic content of the manufactured product has been established under applicable law or regulation; and

(3) all construction materials are manufactured in the United States—this means that all manufacturing processes for the construction material occurred in the United States.

The Buy America preference only applies to articles, materials, and supplies that are consumed in, incorporated into, or affixed to an infrastructure project. As such, it does not apply to tools, equipment, and supplies, such as temporary scaffolding, brought to the construction site and removed at or before the completion of the infrastructure project. Nor does a Buy America preference apply to equipment and furnishings, such as movable chairs, desks, and portable computer equipment, that are used at or within the finished infrastructure project but are not an integral part of the structure or permanently affixed to the infrastructure project.

Initial

FY 2023 DHS Standard Terms and Conditions

Waivers
When necessary, recipients may apply for, and the agency may grant, a waiver from these requirements. Information on the process for requesting a waiver from these requirements is on the website below.

(a) When the Federal agency has made a determination that one of the following exceptions applies, the awarding official may waive the application of the domestic content procurement preference in any case in which the agency determines that:

(1) applying the domestic content procurement preference would be inconsistent with the public interest;

(2) the types of iron, steel, manufactured products, or construction materials are not produced in the United States in sufficient and reasonably available quantities or of a satisfactory quality; or

(3) the inclusion of iron, steel, manufactured products, or construction materials produced in the United States will increase the cost of the overall project by more than 25 percent.

A request to waive the application of the domestic content procurement preference must be in writing. The agency will provide instructions on the format, contents, and supporting materials required for any waiver request. Waiver requests are subject to public comment periods of no less than 15 days and must be reviewed by the Made in America Office.

There may be instances where an award qualifies, in whole or in part, for an existing waiver described at "Buy America" Preference in FEMA Financial Assistance Programs for Infrastructure | FEMA.gov.

The awarding Component may provide specific instructions to Recipients of awards from infrastructure programs that are subject to the "Build America, Buy America" provisions. Recipients should refer to the Notice of Funding Opportunity for further information on the Buy America preference and waiver process.

XXXIII. SAFECOM

Recipients receiving federal financial assistance awards made under programs that provide emergency communication equipment and its related activities must comply with the SAFECOM Guidance for Emergency Communication Grants, including provisions on technical standards that ensure and enhance interoperable communications.

XXXIV. Terrorist Financing

Recipients must comply with E.O. 13224 and U.S. laws that prohibit transactions with, and the provisions of resources and support to, individuals and organizations associated with terrorism. Recipients are legally responsible to ensure compliance with the Order and laws.

XXXV. Trafficking Victims Protection Act of 2000 (TVPA)

Trafficking in Persons.

Recipients must comply with the requirements of the government-wide financial assistance award term which implements Section 106 (g) of the Trafficking Victims Protection Act of 2000 (TVPA), codified as amended at 22 U.S.C. § 7104. The award term is located at 2 C.F.R. § 175.15, the full text of which is incorporated here by reference.

FY 2023 DHS Standard Terms and Conditions

XXXVI. Universal Identifier and System of Award Management

Requirements for System for Award Management and Unique Entity Identifier Recipients are required to comply with the requirements set forth in the government-wide financial assistance award term regarding the System for Award Management and Universal Identifier Requirements located at 2 C.F.R. Part 25, Appendix A, the full text of which is incorporated here by reference.

XXXVII. USA PATRIOT Act of 2001

Recipients must comply with requirements of Section 817 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), which amends 18 U.S.C. §§ 175–175c.

XXXVIII. Use of DHS Seal, Logo and Flags

Recipients must obtain permission from their DHS FAO prior to using the DHS seal(s), logos, crests or reproductions of flags or likenesses of DHS agency officials, including use of the United States Coast Guard seal, logo, crests or reproductions of flags or likenesses of Coast Guard officials.

XXXIX. Whistleblower Protection Act

Recipients must comply with the statutory requirements for whistleblower protections (if applicable) at 10 U.S.C § 2409, 41 U.S.C. § 4712, and 10 U.S.C. § 2324, 41 U.S.C. §§ 4304 and 4310.

Initial