Requirements your company's IT / Email Administrator will need to complete in order to add support for DKIM and DMARC:

1. Add three CNAME records (generated by SendGrid) to your DNS
2. Whitelist the SendGrid IP in your SPF record

Assuming your company can satisfy the above requirements, we need to understand the following before we initiate the set-up for DKIM and DMARC support:

1. Does your organization use SendGrid currently, or do you have any other vendors sending email on your behalf via SendGrid?
2. Do you have any spam/firewall appliances that might reject emails sent on behalf of other email addresses? If so, please add our IP 198.37.147.129 to the whitelist for the appliance.
3. We need to confirm a complete list of email domains that your company uses. Please list them here:
4. Does your company currently use DMARC in any capacity?
   - If so, what policy do you have DMARC set to?
   - If set to 'Reject', can the policy be set to 'None' or 'Quarantine' for the purposes of this beta?

After we receive your response to the above questions, here is what will happen next:

1. Recruiting will send you 3 CNAME records that need to be created in your DNS, and the IP address that should be whitelisted within your SPF record (if you haven't already whitelisted it).
2. After the CNAME records have been added, Recruiting will validate, then flip a setting to begin including a DKIM signature in all outbound Recruiting emails. When recipient servers see this signature, they will look up the new CNAMEs in your DNS and be referred to the corresponding DKIM record housed within SendGrid.
3. After this change, as an initial test we will log into Recruiting and send out emails to various platforms such as Gmail, Yahoo, Hotmail, etc., as well as an address within your company's domain. You are free to test with your own accounts if you'd prefer.
4. If all emails are sent and received successfully, we should be good to go. At this point the HR team should monitor their emails for deliverability and let us know if they run into any issues.

Briefly, here is an outline of what an outbound email flow will look like once we've activated this feature:

1. Recruiting user sends an email out from within Recruiting.
2. Recruiting/Sendgrid attaches a DKIM signature to the header of the email.
3. The recipient email server observes the embedded DKIM signature, checks the associated CNAME records in your DNS, and verifies the signature against the SendGrid registration.
4. DKIM check passes, SPF check passes, and DMARC alignment checks pass (if you use DMARC). Email is considered legitimate.

If you have any questions on any of the above, please contact RecruitingSupport@Paycor.com.